6th ANNUAL DISRUPTIVE TECHNOLOGIES CONFERENCE

"Capability Widening and Adapting to a Global Tech Base"

Washington, DC

14 - 15 October 2009

Agenda

Wednesday 14 October, 2009

DDR&E IMPERATIVES, HOW INDUSTRY CAN HELP

- The Honorable Zachary J. Lemnios, Director, Defense Research & Engineering

GOVERNMENT CTO PANEL: TECHNOLOGY OPPORTUNITIES AND CHALLENGES

Panelists:

- Dr. Thomas Killion, Deputy Secretary of Army (Research & Technology/Chief Scientist)
- Dr. Larry Schuette, Director of Innovation, Office of Naval Research

CAPABILITY GAP CHANGING SURPRISES - AVOIDANCE AND EXPLOITATION

- Dr. Don Wyma, Director for Scientific & Technical Intelligence Analysis Office of the Under Secretary of Defense (Intelligence)

TRACK I: CYBER NETWORK ASSURANCE: OPERATIONS - DEFENSE/ATTACK

- **DEVELOPING SECURITY ARCHITECTURES USING PROTECTED CORE NETWORKING CONCEPTS:** Mr. Dennis McCallam, Principal Architect, Security, Northrop Grumman
- **CYBER WARFARE-GOING ON THE OFFENSE:** Mr. John Kimmins, Executive Director/Fellow, Telecordia Technologies, Inc.

TRACK II: MOBILITY AND TERRAIN/SEA CONTROL: ENERGY, POWER SUPPLY, PROPULSION

****THIS SESSION WILL BE HELD AT THE UNCLASSIFIED LEVEL*

- **NEW PACKAGING AS A CLUTTER REDUCTION METHOD:** Mr. Keith Donaldson, VP Technology, Liberty Packaging Co.,Inc.
- **THE CYCLONE ENGINE AND ITS APPLICATION TO POWERING MANNED AND UNMANNED VEHICLES OR AS AN AUXILIARY POWER UNIT (UNCLASSIFIED):** Dr. Phillip Myers, President, Advent Power Systems
- **REAL-TIME 3D DATA GATHERING, VISUALIZATION, AND DATA FUSION FROM MANNED/UNMANNED PLATFORMS:** Mr. Chris Brown, Business Development Manager, Autonomous Solutions, Inc.

TRACK III: CLOUD COMPUTING, DATA SERVICES, SOCIAL NETWORKS

- **THE BUSINESS CASE FOR A PUBLIC-PRIVATE SECTOR PARTNERSHIP IN HIGH PERFORMANCE COMPUTING:** Dr. Roger Werne, Deputy Director - Industrial Partnerships, Lawrence Livermore National Laboratory
- **SUPER ENPOWERED INDIVIDUALS:** Mr. William Coffey, Director, The Telesti Group
- **OPEN ARCHITECTURE (OA) IS BUSINESS CHANGE:** Mr. Michael McCrave, Military System Engineer, Alion Science and Technology

TRACK IV: ISR—SEE, ACT DECIDE

- **MINIATURIZED, MODULAR, HIGH RESOLUTION X-RAY BACKSCATTER IMAGING AS A BLUE FORCE ENHANCER,** Mr. William Baukus, Director, Technology Development, American Science and Engineering, Inc.
- **COUNTERSPACE CAPABILITIES USING SMALL SATELLITES: BRIDGING THE GAP IN SPACE SITUATIONAL AWARENESS:** Dr. Rick Mullikin, Business Development Manager, Lockheed Martin IS&GS

Thursday 15 October, 2009

JOINT CAPABILITY AREAS*

TRACK V

- Mr. John Neri: Battlespace Awareness
- COL William Hickman: Command and Control
- CAPT Ken Bowen: Net-Centric:

TRACK VI

- CAPT William Campbell, J8 FAD: Force Application and Support
- Mr. Steve Inada: Protection
- Lt COL Lisa Hess: Logistics

CLOSING PANEL: SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF) CHALLENGES AND SOLUTIONS
****THIS SESSION WILL BE HELD AT THE UNCLASSIFIED LEVEL*

Moderator: Mr. Warren Amason, Senior Vice President, Grubb and Ellis

Panelists:

- Mr. Jason Phillippe, Director, Intelligence Programs and Operations, Copper River Information Technology

NDIA
National Defense Industrial Association

PROMOTING NATIONAL SECURITY SINCE 1919

6TH ANNUAL DISRUPTIVE TECHNOLOGIES CONFERENCE

This conference will be held at the SECRET/US level.

"Capability Widening and Adapting to a Global Tech Base"

Convened by the C4ISR Division of NDIA
In Collaboration with the Office of the Director, Defense Research and Engineering

WHAT YOU DON'T WANT TO MISS AT THIS CONFERENCE:

- Technologies that possess intrinsic benefits that:
  - alter warfighter operations
  - create game changing military capabilities
- Joint Staff Functional Capability Board identified gaps and desired operational capability needs
- A one of a kind panel seeking to unravel the "mystery" behind SCIF technical features, construction costs, reusability, and much, MUCH more!

FEDERAL GATEWAY ▸ NAVY YARD METRO ▸ 1100 NEW JERSEY AVENUE, WASHINGTON, DC

OCTOBER 14 - 15, 2009

EVENT #0920

WWW.NDIA.ORG/MEETINGS/0920

INTRODUCTION

Military doctrine is evolving from 'network centric warfare' to 'knowledge centric warfare', where the focus is on decentralized usage of 'higher level' knowledge of evolving social structures and information networks. As military operations increasingly move beyond symmetric kinetic warfare scenarios to embrace peacekeeping and counterinsurgency functions, their operational success will increasingly depend on the ability to harness the latent knowledge embedded in the evolutionary behavior (in both the real world and cyberspace) of individuals and social groups (military personnel, militia members and civilians). An increasing 'sensor-networked' physical world (e.g., Webcams on bridges, real-time traffic feeds, Google Map street-views) and a progressively 'participatory' demographic profile (expressed through the willingness to share images, opinions and real-time updates via technologies such as Facebook and Twitter) present both significant opportunities and serious challenges.

On the positive side, these disruptive technological trends offer the military unprecedented opportunities to exploit the 'power of the network'-sophisticated social and information network mining tools may be used to isolate key adversarial actors and gain a more detailed understanding of relevant activity patterns. On the flip side, these same technologies can be used by adversaries to learn and adapt to military tactics (e.g., using SMS broadcasts to alert sympathetic tribesmen or monitoring Webcams to learn troop movement patterns). In addition, the information content in a 'participatory' information network is also of widely varying fidelity-effective military invention, especially in civilian environments, mandates a reliance on near-real time, approximate analysis of the content embedded in very large, complex social and information networks.

This conference will address why military C2 practices and technologies will need revolutionary advances in two key areas in order to contend with the emergence of an increasingly sensor-rich, participatory, information grid:

1) Development of technologies that exploit the power of sensor-driven and participatory information systems, but can effectively 'interrupt', 'limit' or 'delay' the availability of such information to the adversary.

2) Adoption of decision architectures that exploit the responsiveness that arises from pushing decision-making to the 'edge', but that can contend with the higher degree of uncertainty and conflicting knowledge that results from the rapid, automated analysis of content in such decentralized information networks.

CONFERENCE OBJECTIVES

The NDIA C4ISR Division will convene the 6th Annual Disruptive Technologies Conference as a forum of discussion and opportunity for government and industry senior technologists, product engineers and strategists to focus upon technology enduced game changing military capabilities. Avenues to proficiently deliver these new capabilities into the warfighters' hands will also be discussed.

Conference Goal: To enable rapid development and fielding of new warfighting capability.

SECRET/US Attendees.

WEDNESDAY, OCTOBER 14, 2009

THIS CONFERENCE WILL BE HELD AT THE SECRET/US LEVEL. ALTHOUGH PRESENTATION MATERIALS WILL BE UNCLASSIFIED, ORAL PRESENTATIONS MAY BE SECRET/US. CLASSIFIED DISCUSSIONS WILL BE LIMITED TO THE DESIGNATED MEETING ROOMS.

7:00 AM — REGISTRATION & CONTINENTAL BREAKFAST

8:00 AM — WELCOME REMARKS AND INTRODUCTIONS

- Mr. Sam Campagna, *Director, Operations, NDIA*
- Dr. Steve Kimmel, *Chairman, NDIA C4ISR Division; Senior Group Vice President, Alion Science & Technology*

8:10 AM — DDR&E IMPERATIVES, HOW INDUSTRY CAN HELP

- The Honorable Zachary J. Lemnios, *Director, Defense Research & Engineering*

8:40 AM — EXPANDING NATIONAL SECURITY TECHNOLOGIES & CAPABILITIES

Keynote Speaker:
- Dr. Regina E. Dugan, *Director, DARPA*

9:20 AM — GOVERNMENT CTO PANEL: TECHNOLOGY OPPORTUNITIES AND CHALLENGES

Panel Lead:
- Mr. Frank Cooper, *Vice President and Chief Technical Officer, Concurrent Technologies Corporation*

Panelists:
- Dr. Thomas Killion, *Deputy Secretary of Army (Research & Technology/Chief Scientist)*
- Dr. Scott P. Sarlin, *Director of Science and Technology (Acting), Office of the Director of National Intelligence*
- Ms. Michele Weslander, *Office of the Director of National Intelligence (ODNI)*
- Dr. Larry Schuette, *Director of Innovation, Office of Naval Research*

10:15 AM — BREAK

10:30 AM — CAPABILITY GAP CHANGING SURPRISES - AVOIDANCE AND EXPLOITATION

- Dr. Don Wyma, *Director for Scientific & Technical Intelligence Analysis Office of the Under Secretary of Defense (Intelligence)*

11:15 AM — INDUSTRY CTO PANEL: PRODUCTIZING IRAD RESULTS

Panel Lead:
- Mr. Keith Masback, *President, US Geospatial Intelligence Foundation*

Panelists:
- Mr. Paul R. Davis, *Senior Vice President and Chief Technology Officer, NJVC, LLC*
- Mr. Ed Zoiss, *Director, Research & Development, Harris Corp*
- Mr. Brian O'Toole, *Chief Technology Officer, GeoEye*
- Mr. Robert "Jeff" Morris, *Vice President, M&CSS Engineering, LMCO*

12:15 PM — LUNCH

1:00 PM — BREAKOUT TRACKS: EMERGING DISRUPTIVE TECHNOLOGIES

AGENDA: OCTOBER 14

TRACK I
CYBER NETWORK ASSURANCE: OPERATIONS - DEFENSE/ ATTACK

Track I Leader:

- Mr. Tony Bogovic, *Assistant Vice President, Applied Research Organization, Telecordia Technologies, Inc.*

1:00 PM
DEVELOPING SECURITY ARCHITECTURES USING PROTECTED CORE NETWORKING CONCEPTS
- Mr. Dennis McCallam, *Principal Architect, Security, Northrop Grumman*

1:30 PM
CYBER WARFARE-GOING ON THE OFFENSE
- Mr. John Kimmins, *Executive Director/Fellow, Telecordia Technologies, Inc.*

2:00 PM
CYBER TRADECRAFT & OPSEC: TECHNIQUES AND TECHNOLOGIES TO RETAKE THE INTERNET HIGH GROUND
- Mr. Lance Cottrell, *Chief Scientist, Anonymizer, Inc. - Abraxas Corporation*

TRACK II
MOBILITY AND TERRAIN/SEA CONTROL: ENERGY, POWER SUPPLY, PROPULSION

THIS SESSION WILL BE HELD AT THE UNCLASSIFIED LEVEL

Track II Leader:

- Mr. Robert Baker, *Deputy Director, Plans & Programs, Office of the Director of Defense Research & Engineering*

1:00 PM
NEW PACKAGING AS A CLUTTER REDUCTION METHOD
- Joe Spitz, *Vice President, Liberty Packaging Co., Inc.*
- Mr. Keith Donaldson, *VP Technology, Liberty Packaging Co., Inc.*

1:30 PM
THE CYCLONE ENGINE AND ITS APPLICATION TO POWERING MANNED AND UNMANNED VEHICLES OR AS AN AUXILIARY POWER UNIT (UNCLASSIFIED)
- Dr. Phillip Myers, *President, Advent Power Systems*

2:00 PM
REAL-TIME 3D DATA GATHERING, VISUALIZATION, AND DATA FUSION FROM MANNED/UNMANNED PLATFORMS
- Mr. Chris Brown, *Business Development Manager, Autonomous Solutions, Inc.*

TRACK III
CLOUD COMPUTING, DATA SERVICES, SOCIAL NETWORKS

Track III Leader:

- Mr. John Scott, *Director, Mercury Federal Systems*

2:30 PM
THE BUSINESS CASE FOR A PUBLIC-PRIVATE SECTOR PARTNERSHIP IN HIGH PERFORMANCE COMPUTING
- Dr. Roger Werne, *Deputy Director - Industrial Partnerships, Lawrence Livermore National Laboratory*

3:00 PM
SUPER ENPOWERED INDIVIDUALS
- Mr. William Coffey, *Director, The Telesti Group*

3:30 PM
OPEN ARCHITECTURE (OA) IS BUSINESS CHANGE
- Mr. Michael McCrave, *Military System Engineer, Alion Science and Technology*

TRACK IV
ISR—SEE, ACT DECIDE

Track IV Leader:

- Mr. Sam Chun, *Director Solutions, EDS/HP*

2:30 PM
MINIATURIZED, MODULAR, HIGH RESOLUTION X-RAY BACKSCATTER IMAGING AS A BLUE FORCE ENHANCER
- Mr. William Baukus, *Director, Technology Development, American Science and Engineering, Inc.*

3:00 PM
COUNTERSPACE CAPABILITIES USING SMALL SATELLITES: BRIDGING THE GAP IN SPACE SITUATIONAL AWARENESS
- Dr. Rick Mullikin, *Business Development Manager, Lockheed Martin IS&GS*

3:30 PM
CARBON NANOTUBE (CNT) COMPOSITES USING SOLUTION SPUN FIBERS
- Dr. Amy Heintz, *Principal Research Scientist, Battelle Memorial Institute*

4:00 PM WEDNESDAY SESSION COMPLETE

THURSDAY, OCTOBER 15, 2009

7:00 AM — REGISTRATION & CONTINENTAL BREAKFAST

8:00 AM - 11:00 AM — JOINT CAPABILITY AREA: COCOM PERSPECTIVE
The following Tracks and JCA sessions will provide a forum for Joint Staff Functional Capability Board representatives to discuss capability gaps and associated desired operational capabilities.

JOINT CAPABILITY AREAS*

SECRET/NO FOREIGN

TRACK V

Track V Leader:
CDR Chris Nash, *Joint Staff, J8*

8:00 AM
Mr. John Neri: Battlespace Awareness: The ability to understand dispositions and intentions as well as the characteristics and conditions of the operational environment that bear on national and military decision-making.

8:30 AM
COL William Hickman: Command and Control: The ability to exercise authority and direction by a properly designated commander or decision maker over assigned and attached forces and resources in the accomplishment of the mission.

9:00 AM
CAPT Ken Bowen: Net-Centric: The ability to provide a framework for full human and technical connectivity and interoperability that allows all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it.

9:30 AM
Mr. Harry Argo (Cancelled): Building Partnerships: The ability to set the conditions for interaction with partner, competitor or adversary leaders, military forces, or relevant populations by developing and presenting information and conducting activities to affect their perceptions, will, behavior, and capabilities.

10:00 AM
General Discussion

TRACK VI

Track VI Leader:
Mr. Mike Knollman, *Assistant Deputy Under Secretary of Defense Acquisition, Technology and Logistics (Joint/Coalition Operation Support)*

8:00 AM
CAPT William Campbell, J8 FAD: Force Application: The ability to integrate the use of maneuver and engagement in all environments to create the effects necessary to achieve mission objectives.

8:30 AM
CAPT William Campbell, J8 FAD: Force Support: The ability to establish, develop, maintain and manage a mission ready Total Force, and provide, operate, and maintain capable installation assets across the total force to ensure needed capabilities are available to support National security.

9:00 AM
Mr. Steve Inada: Protection: The ability to prevent/mitigate adverse effects of attacks on personnel (combatant/non-combatant) and physical assets of the United States, allies and friends.

9:30 AM
Lt COL Lisa Hess: Logistics: The ability to project and sustain a logistically ready joint force through the deliberate sharing of national and multi-national resources to effectively support operations, extend operational reach and provide the joint force commander the freedom of action necessary to meet mission objectives.

10:00 AM
General Discussion

* JOINT CAPABILITY AREAS...

- are comprised of functional portfolios to focus management and resource attention upon a desired capability-based vice threat-based envisioned and synchronized military force development and planning enterprise.
- encompass capability needs definition, gap and excess analysis, major trade analyses, and capabilities planning, i.e., the DoD military capability divided into manageable functional entities.
- provide a framework to enable a capabilities-based US military enterprise to focus on emerging technological opportunities that certain capabilities such as long-range precision strike; transformed maneuver and expeditionary forces; and systems to overcome anti-access and area-denial threats.
- enable and anticipate the diverse range that any adversary might employ and the necessary US military responsive mix of technology-system-operational capabilities required to resolve such.

10:30 AM

CLOSING PANEL: SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF) CHALLENGES AND SOLUTIONS

THIS SESSION WILL BE HELD AT THE UNCLASSIFIED LEVEL

This one-of-a-kind panel seeks to unravel the "mystery" behind SCIF technical features, certification, construction costs, reusability, etc. and much, much more!

Moderator:
- Mr. Warren Amason, *Senior Vice President, Grubb and Ellis*

Panelists:
- Mr. Jason Phillippe, *Director, Intelligence Programs and Operations, Copper River Information Technology*
- Mr. Joseph D. Cooper, *President, SCIF Contractors Association*

11:00 AM

WRAP-UP

- Dr. Steve Kimmel, *Chairman, NDIA C4ISR Division; Senior Group Vice President, Alion Science & Technology*

11:15 PM

ADJOURN

PROMOTIONAL PARTNERSHIP

Increase your company or organization's exposure at this premier event by becoming a Promotional Partner. For this conference, we are offering three promotional tiers:

SILVER	GOLD	PLATINUM
$1,000	$2,500	$5,000
		2 Complimentary Attendees
	Company Logo on Materials	Company Logo on Materials
Breakfast or Break Sponsorship Signage	Reception Sponsorship Signage	Main Podium Recognition at Conference

For more information, please contact Sam Campagna at (703) 247-2544 or scampagna@ndia.org

ATTIRE

Appropriate attire for the conference is business suit for industry and class A uniform of the day for military.

TRAVEL INFORMATION

Metro Rail (Preferred):

The Green Line's Navy Yard Metro Station is located directly across from the Federal Gateway (1100 New Jersey Avenue). For Metro schedules and fare information go to: http://www.wmata.com/

Parking:

Area street parking is limited. Metro is suggested.

From Ronald Reagan National Airport:

Take George Washington Parkway North to Interstate 395 North. Then follow Northern VA directions provided below.

From Northern VA:

Take Interstate 395N across the 14th St. Bridge. Stay Right and follow signs to the South Capitol St. exit. Stay to the right and exit right at South Capitol St. Continue through the first traffic light and stay to the right (the two left lanes pass under M St.). Turn left at the next traffic light, M St. SE. Go three blocks and Federal Gateway is on your left.

From Southern MD:

Take Interstate 295 North across the South Capital St. Bridge. Stay to the right (the two left lanes pass under M St.) until you reach the fifth street. Turn Right on M St. SE and Federal Gateway is three blocks down on your left.

PROCEEDINGS

Unclassified proceedings will be made available after the conference.

CONTACTS

Ms. Taryn Crowder
Meeting Planner:
tcrowder@ndia.org
(703) 247-2566

Dr. Steve Kimmel,
Conference Chair:
skimmel@alionscience.com
(703) 269-3465

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION
2111 WILSON BOULEVARD, SUITE 400
ARLINGTON, VA 22201-3061
(703) 247-2566
(703) 522-1885 FAX
WWW.NDIA.ORG

6TH ANNUAL DISRUPTIVE TECHNOLOGIES CONFERENCE

This conference will be held at the SECRET/US level.

FOR INFORMATION, VISIT:
WWW.NDIA.ORG/MEETINGS/0920



Disruptive Technology Conference

CAPT Ken Bowen

J68

15 October 2009



- Task: Brief Net-Centric Equities as they relate to COCOM Gaps and Joint Capability Areas.

Purpose: Examine near and long term solutions for challenges that will continue to manifest over the next twenty years

- Topics:
  - JCAs
  - COCOM Capability Gap Analysis (CGA)
  - Individual JCA / Gap Focus
  - Game Changing capabilities

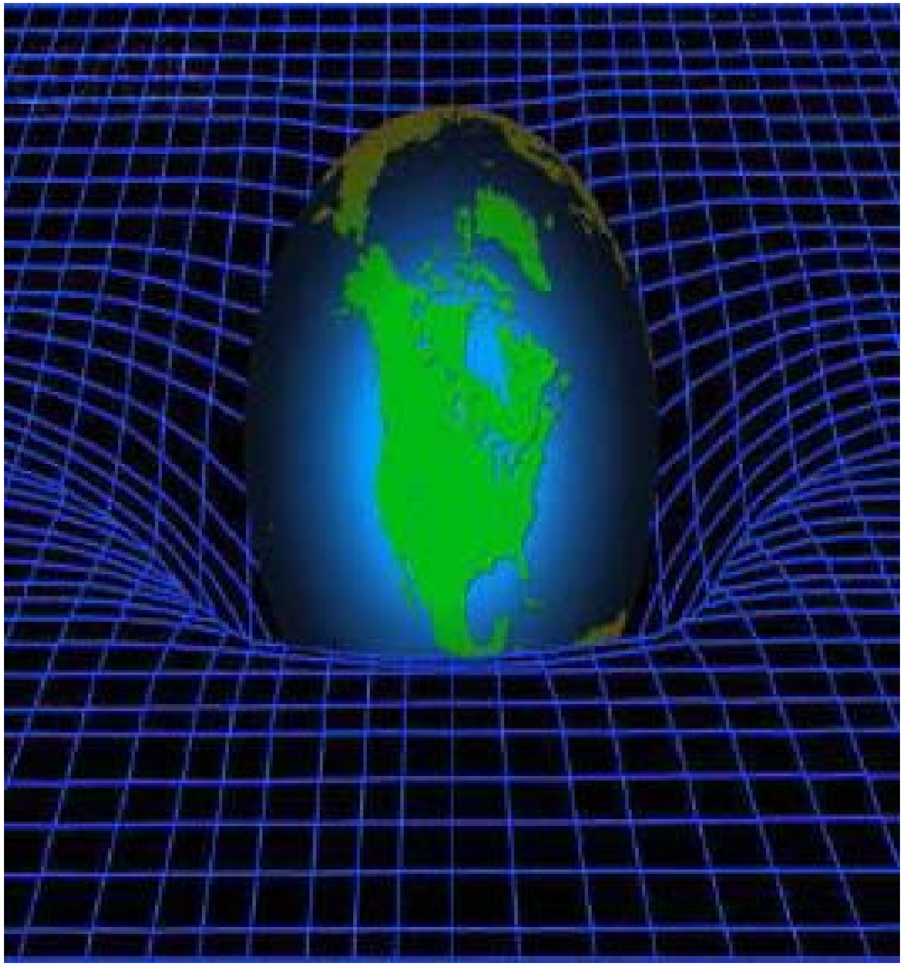
Near Term

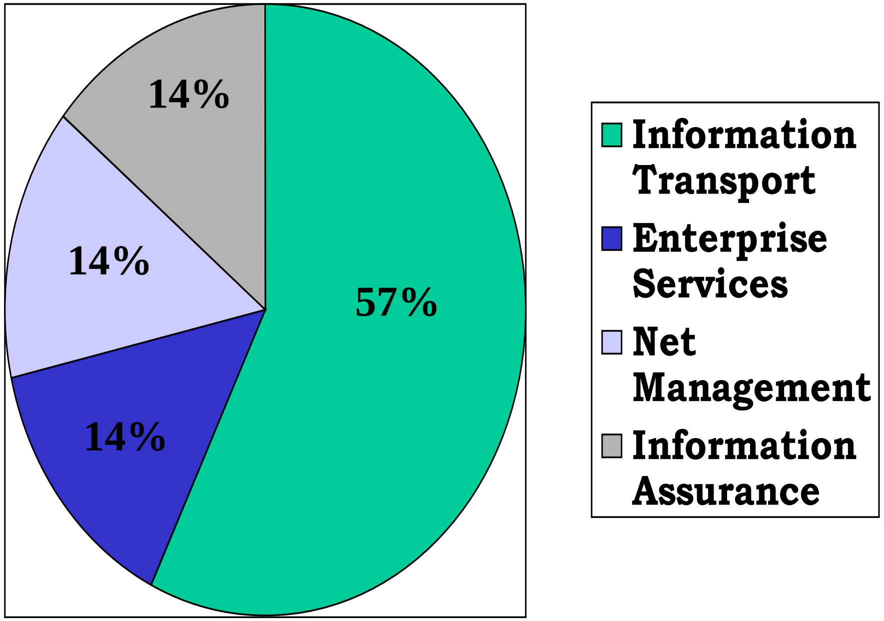
Long Term

- **Tier One: Net Centric**

  Tier Two:

    - Information Transport
    - Enterprise Services
    - Net Management
    - Information assurance





- **35 COCOM Shortfalls**
- **7 synthesized Gaps**
- **57% of Warfighter's Net Centric needs reside in Information Transport**
- **Initial Submissions for FY10 are very representative of FY 09**

- **Mission Focus:**
  - **Continue to connect disparate legacy networks, work on infrastructure and build toward commonality on battlefield**
- **Problem Space:**
  - **C2/Comm OTM, BLOS, Legacy disparate networks.**

- **Mission Focus:**
  - Provide all partners access to appropriate levels of information to speed mission success
- **Problem Space:**
  - Lack of ability to share information among Service, Coalition, National, and Ad-hoc partners

OB-1

CENTRIX

Public Key Infrastructure

Multi Nation Info Sharing

- **Mission Focus:**
  - Provide Network redundancy and transparency to the warfighter.
- **Specific Equities:**
  - Lack of SATCOM in various theaters/areas of operation

- **Mission Focus:**
  - Provide a Battle space quality situational awareness to the cyber environment.

- **Specific Equities:**
  - Lack of JTF or COCOM Commander to have real-time Cyber situational Awareness

Information Transport:

- More bandwidth with bigger pipes or new data compression technology

Enterprise Services:

- All Domains to the right users at the right place with the smallest infrastructure

Net Management:

- Dynamic allocation of bandwidth and spectrum

Information Assurance:

- Active GiG environment that is self healing and policing, before, during, and after an event.

Questions

Applications of Real-Time 3D Visualization & World-Building

Chris Brown
Business Development Manager
Autonomous Solutions, Inc.
Petersboro, Utah

AUTONOMOUS SOLUTIONS

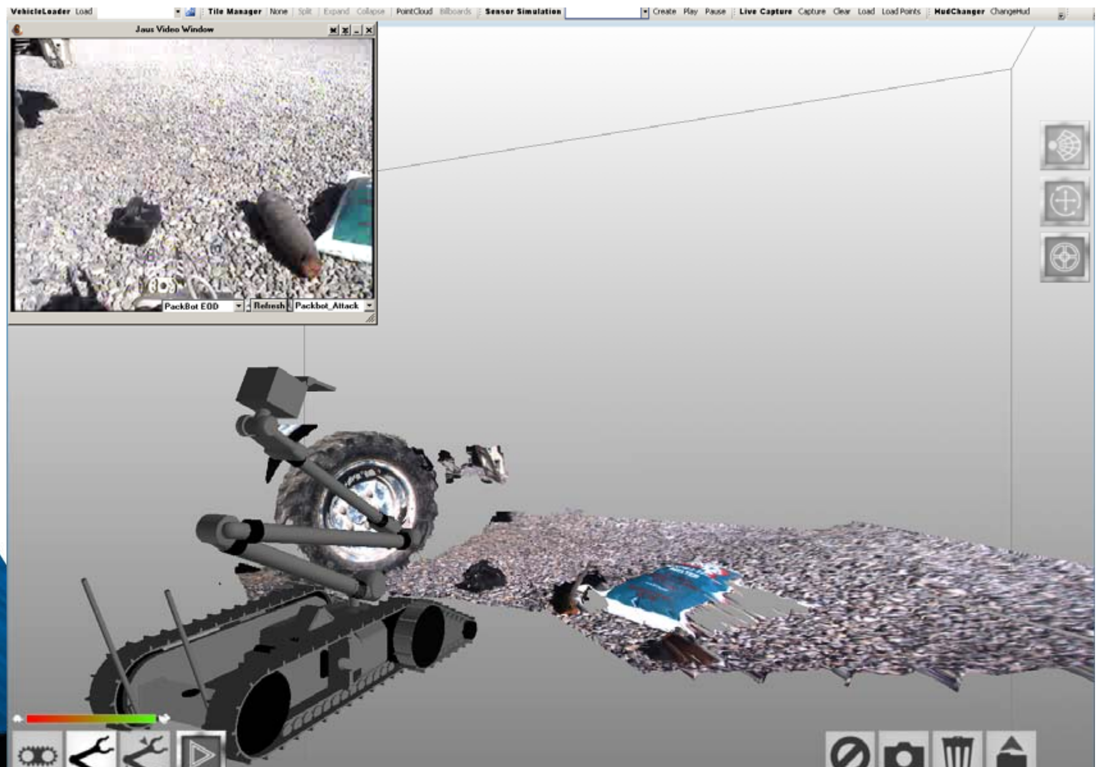
Company Overview

- Company Started in 2000 with John Deere
- Located in Petersboro, Utah
- Established business in military, mining, and agriculture markets
- Business from autonomous vehicles for end users to advanced R&D in robotics

AUTONOMOUS SOLUTIONS

Advanced R&D – 3D Visualization

- Capture 3D data fast (stereovision, lidar, etc)
- Apply texture to point cloud (ie, make it look like a 3D photo)
- Place robot in the view



AUTONOMOUS SOLUTIONS

3D Visualization - Applications

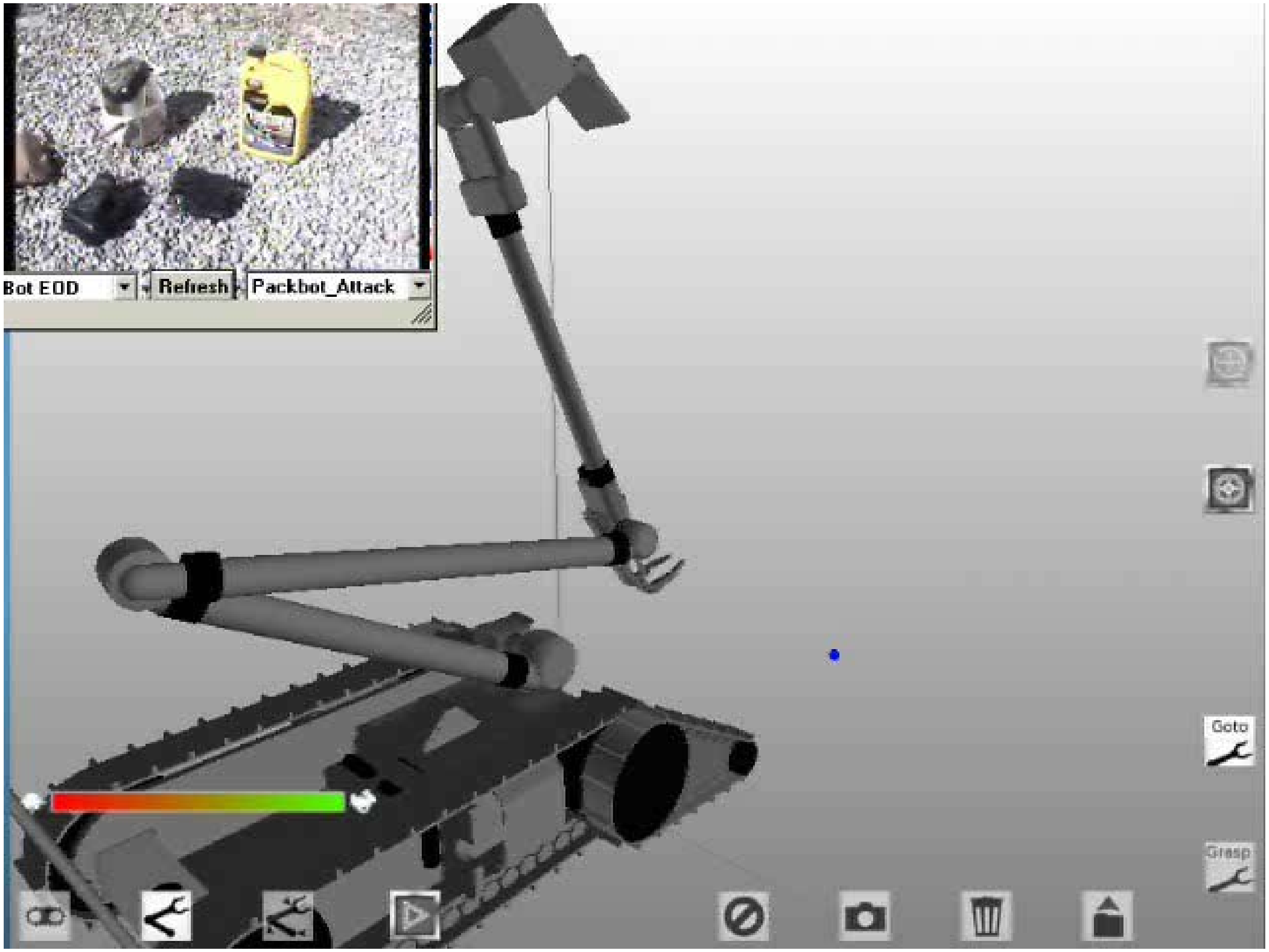
- Robotic Manipulation
  - Enhance depth perception
- Robotic Mobility
  - Characterize terrain/surroundings
  - Enabling technology for autonomy
- Mapping (Robotic or Manned)
  - Efficient searching
  - Situational Awareness
  - Information sharing
- Change Detection (Robotic or Manned)
  - Large or small scale

AUTONOMOUS SOLUTIONS

Initial Impetus - Current EOD Operations

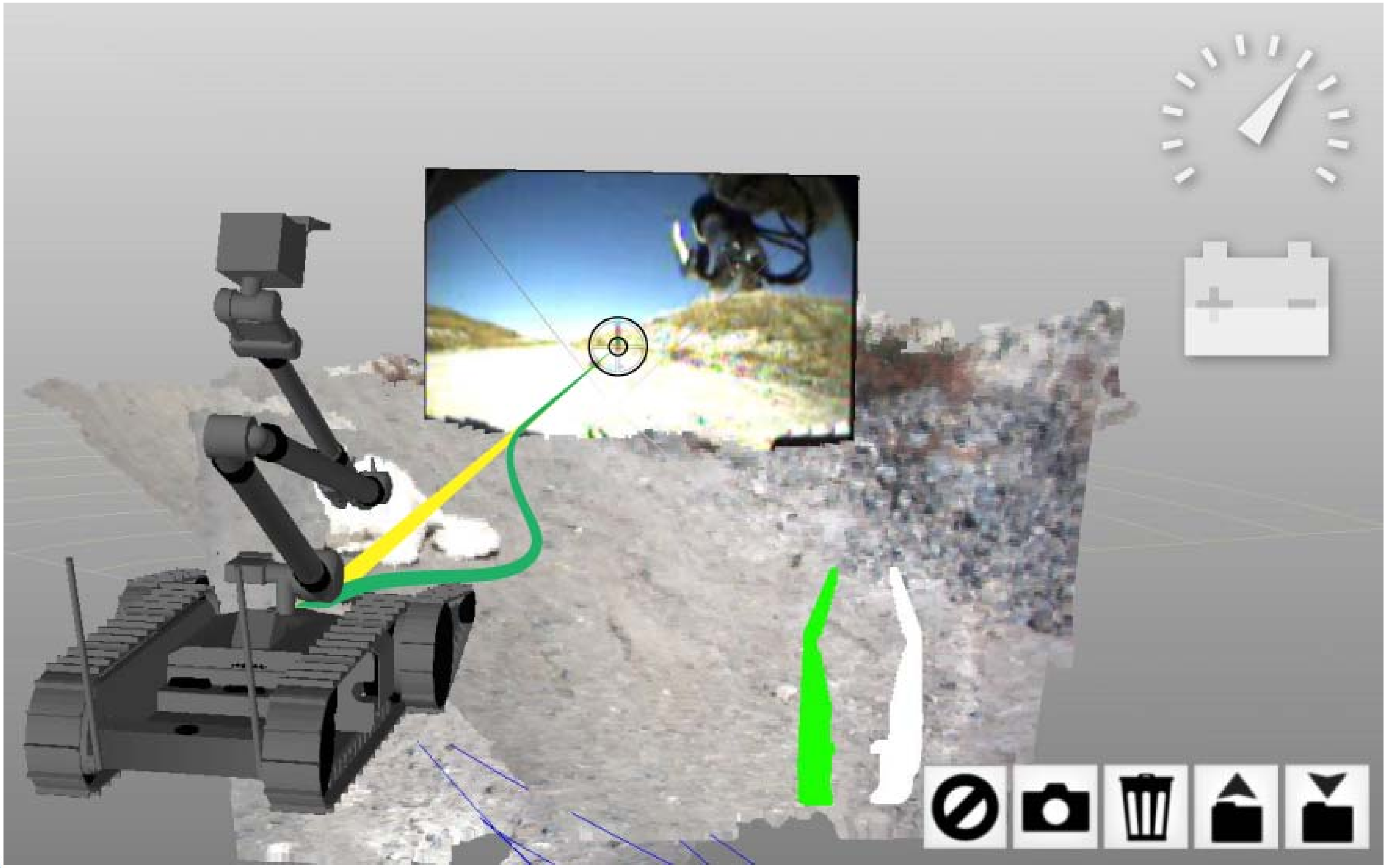
- Lack of depth perception
- Lack of a sense of scale
- Inability to see parts of the robot in the world around it
- Confusion of context
- Want a “God’s-eye view”

Enhancing Depth Perception



AUTONOMOUS SOLUTIONS

Improving Mobility & Enabling Autonomy



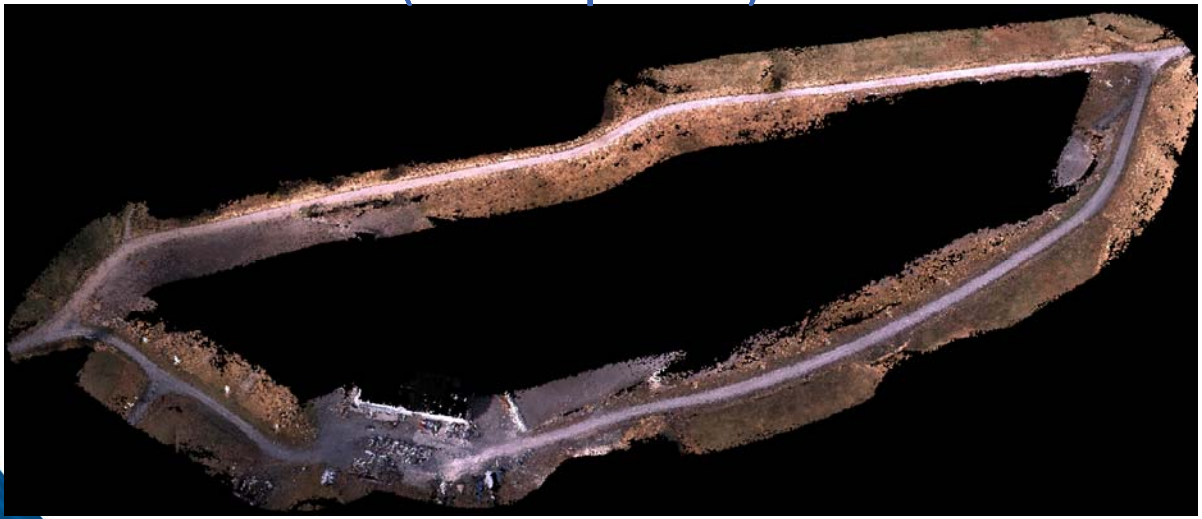
AUTONOMOUS SOLUTIONS

Mapping & Situational Awareness

AUTONOMOUS
SOLUTIONS

Data Fusion & Change Detection

A Priori data (aerial photo)



Real-time data (human driven)

Data Fusion & Change Detection

Fused Data

3D Visualization – Technology Challenges

- Sensors
  - Get accurate, high resolution data fast
- Visualization
  - Render for the user fast, apply texture
- Data management
  - Render at different resolutions, memory management
- Data registration
  - Fusing a priori and real time data, different scales, resolutions, accuracies

AUTONOMOUS SOLUTIONS

Force Application and Force Support Functional Capabilities Boards (FA FCB/FS FCB)

CAPT Bill Campbell

6th NDIA Disruptive Technologies Conference

15 Oct 09

Agenda

- FA FCB Portfolio
- FS FCB Portfolio
- What Keeps Us Up at Night

FA FCB Portfolio

Force Application FCB: Identify, assess and prioritize programmed, projected and potential force application capability needs

- **Maneuver**
  - Land combat operations
  - Maritime combat operations
  - Air combat operations
  - Space combat operations

- **Engagement – Kinetic**
  - Conventional attack
  - Nuclear attack
  - Close combat
  - Joint fire support

- **Engagement – Non-kinetic**
  - EA/DE
  - Computer network attack

FS FCB Portfolio

Tier 1

Force Support

Tier 2

Force Management

Tier 3
- Global Force Management
- Force Configuration
- Global Posture Execution

Example Actions/ Issues
- *GFM – Data Initiative*
- *Defense Readiness Reporting System (DRRS)*
- *Cyber DCR*

Force Preparation

Tier 3
- Training
- Exercising
- Educating
- Doctrine
- Lessons Learned
- Concepts
- Experimentation

Example Actions/ Issues
- *Language and Culture*
- *Operationalizing the Reserve*
- *Joint C4 Planners Course*

Human Capital Management

Tier 3
- Personnel and Family Support
- Personnel Management

Example Actions/ Issues
- *Support to Families*
- *Grow the Force*
- *Manpower*
- *Joint Personnel Accountability Assessment*
- *Joint Manpower Validation Process*

Health Readiness

Tier 3
- Health Care Delivery
- Health Service Support
- Force Health Protection

Example Actions/ Issues
- *TRICARE Benefit Reform*
- *Healthcare Facilities Recapitalization*

What keeps us up at night … Red disruptive technologies & capabilities

- Electronic attack
- Cyber threats
- Maritime surface & subsurface threats
- Mobile, fleeting targets
- Urban operations
- Space control

NORTHROP GRUMMAN

Applying Protected Core Networking Concepts to Develop a Protected Trust Based Security Environment

Dennis McCallam
Principal Architect, Security
Northrop Grumman Corporation
October 2009

Agenda

- Current State of things
  - What about the threat
  - What are the problems we are trying to address
- A description of a Protected Core Network
  - As it relates to NATO coalitions
  - Why it is foundational to trust based security environments
- Features of a Protected Core Based Security Environment
  - Common services and a reference model
  - Deep dive on authentication

Protected Core Networking Improves Security

NORTHROP GRUMMAN

- **NATO's next generation concept of coalition warfare**

- **A Protected Core is a transport network that:**
  - Offers transport service to users and primarily HIGH availability
  - Includes support for quality of service, priority handling, and security
  - Maintains service, even in situations with directed attacks
  - Set of Protected Core Segments working together (federated)

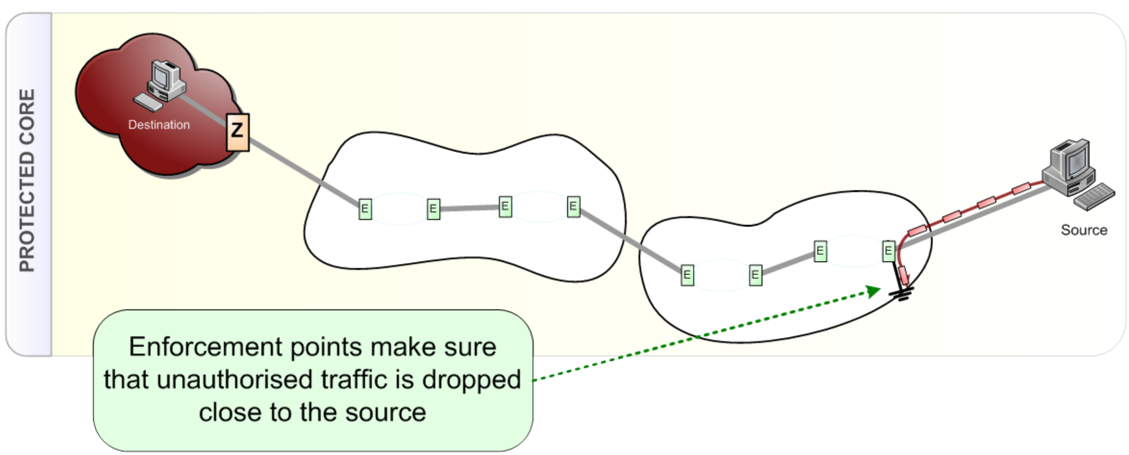
- Assumes security is handled by segment owners

- Its' all about Availability, not Confidentiality and Integrity

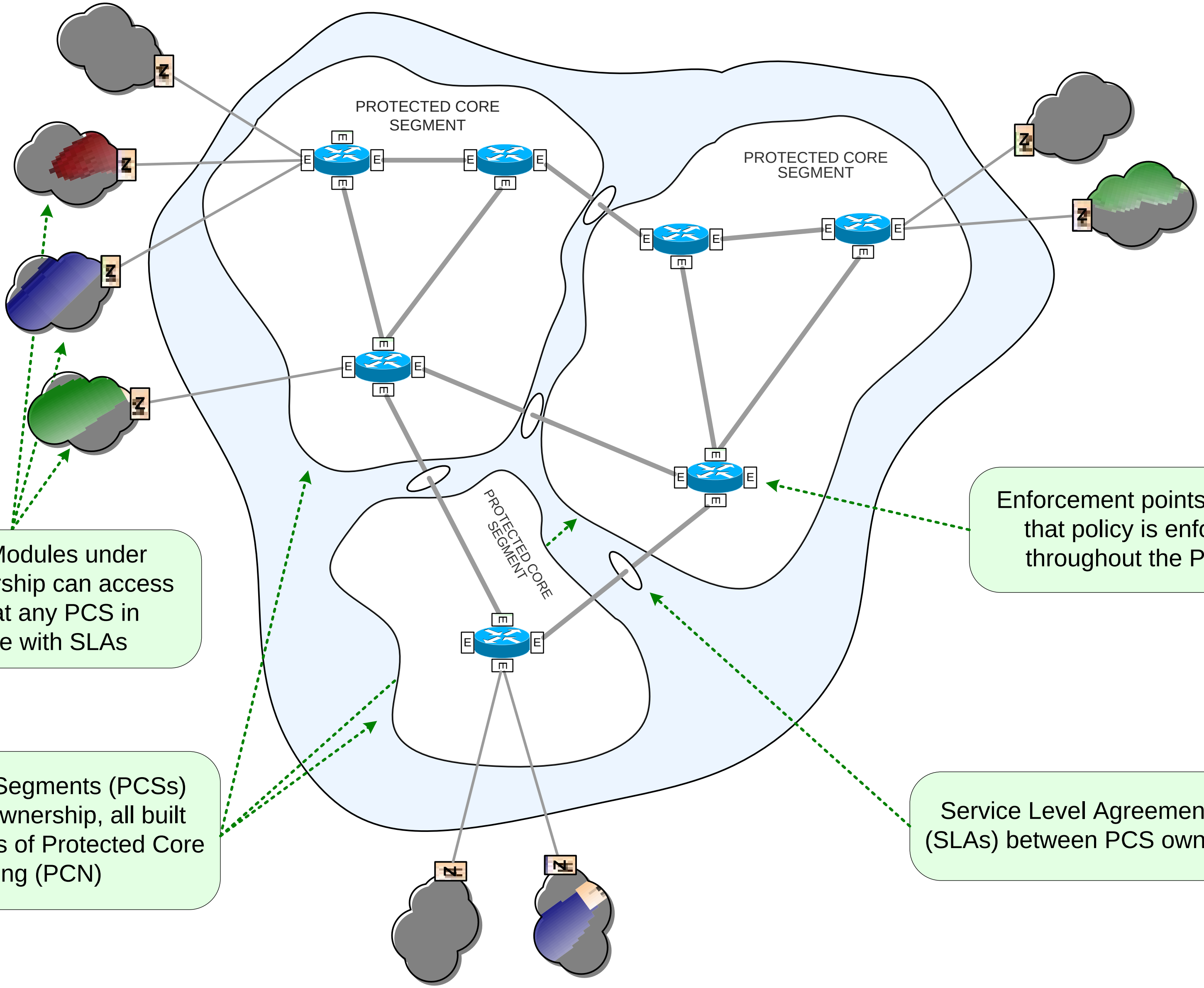
Supports future military operations based on network enabled capabilities by providing the highest service availability.

Definitions – How to construct a PCN

- The concept of Protected Core Networking:
  - Provide transport services in dynamic environments, focus on availability.
  - Utilizes multiple classes of network services for performance and security, and protection of all network components.
- A Protected Core Segment:
  - A network built on PCN working with other Protected Core Segments through Federation of Systems approach.
- A Protected Core:
  - Set of Protected Core Segments working together (federated) to achieve characteristics of Protected Core Networking.



An Example PCore



Consumer Modules under different ownership can access the PCore at any PCS in accordance with SLAs

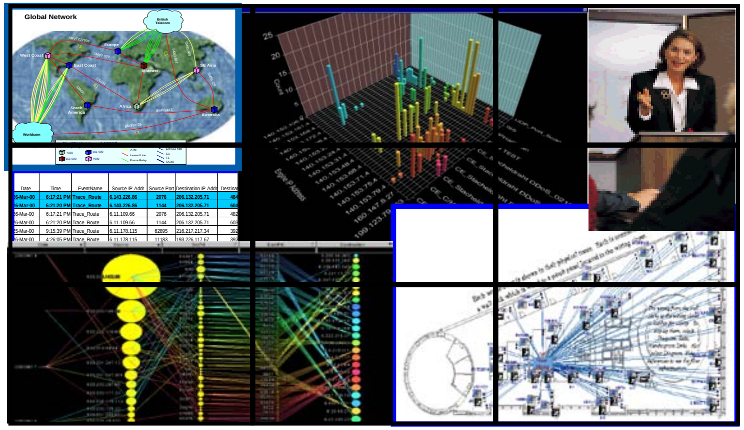
Protected Core Segments (PCSs) under different ownership, all built upon the principles of Protected Core Networking (PCN)

Enforcement points ensure that policy is enforced throughout the PCore

Service Level Agreements (SLAs) between PCS owners

Claims about applying PCN Concepts

- View this as an enterprise architecture framework
- Federated model widens attack surface
- Architecture built on trust, alleviates the need for some decisions……bake trust in
- Can develop autonomous yet integrated zones, a biological (even Borg) model
- “Value” of security is no longer linear
- Add Confidentiality and Integrity back in

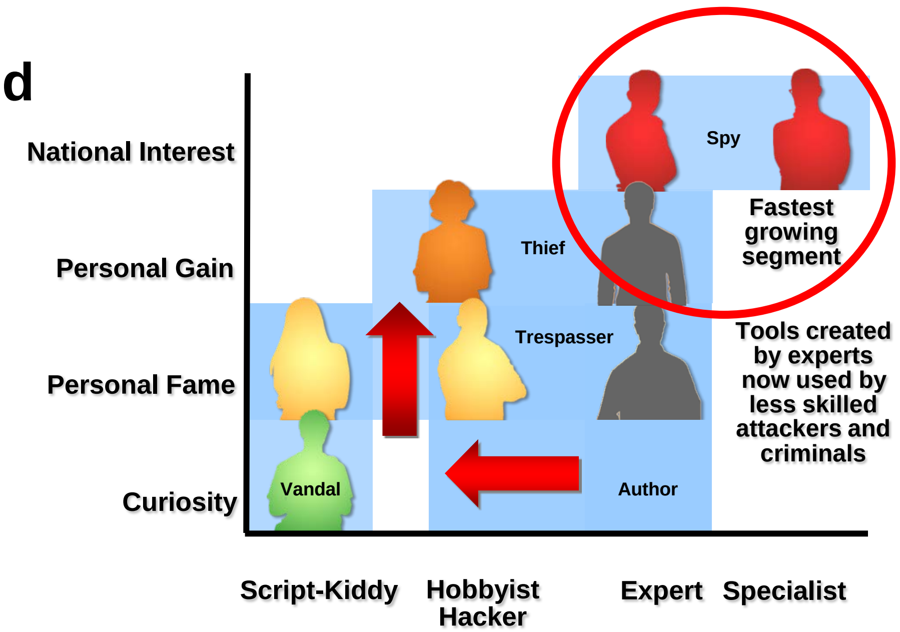


Changing Threats To Data Security

NORTHROP GRUMMAN

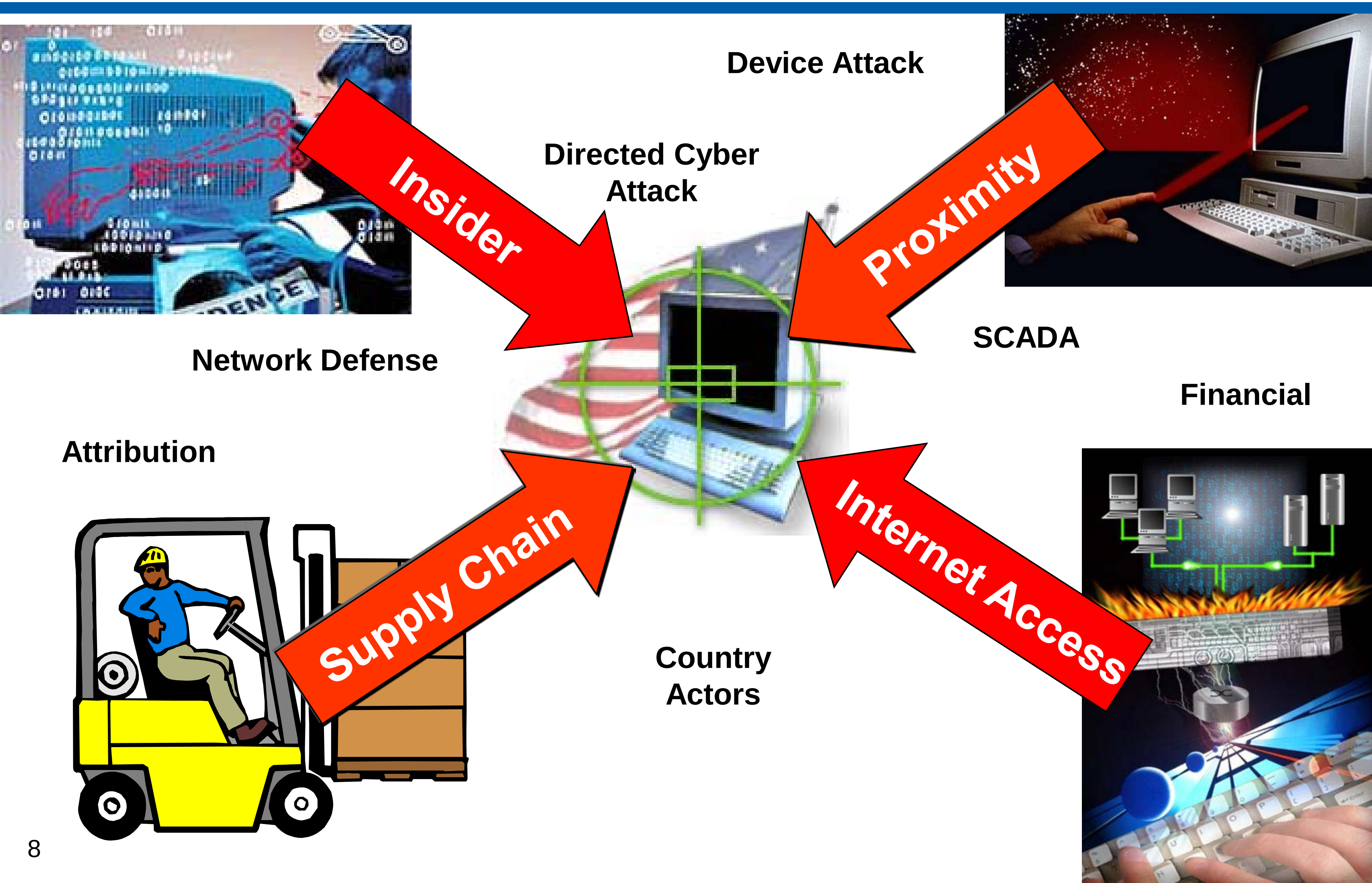
The threat landscape has changed dramatically:

- They are persistent, sophisticated, and in some cases State sponsored
- Firewalls and intrusion detection devices can no longer keep the adversaries out of private networks
- They use common services that must be kept open on the firewalls in order for business to function
- They enlist the end user's unwitting cooperation in order to insert themselves into the network



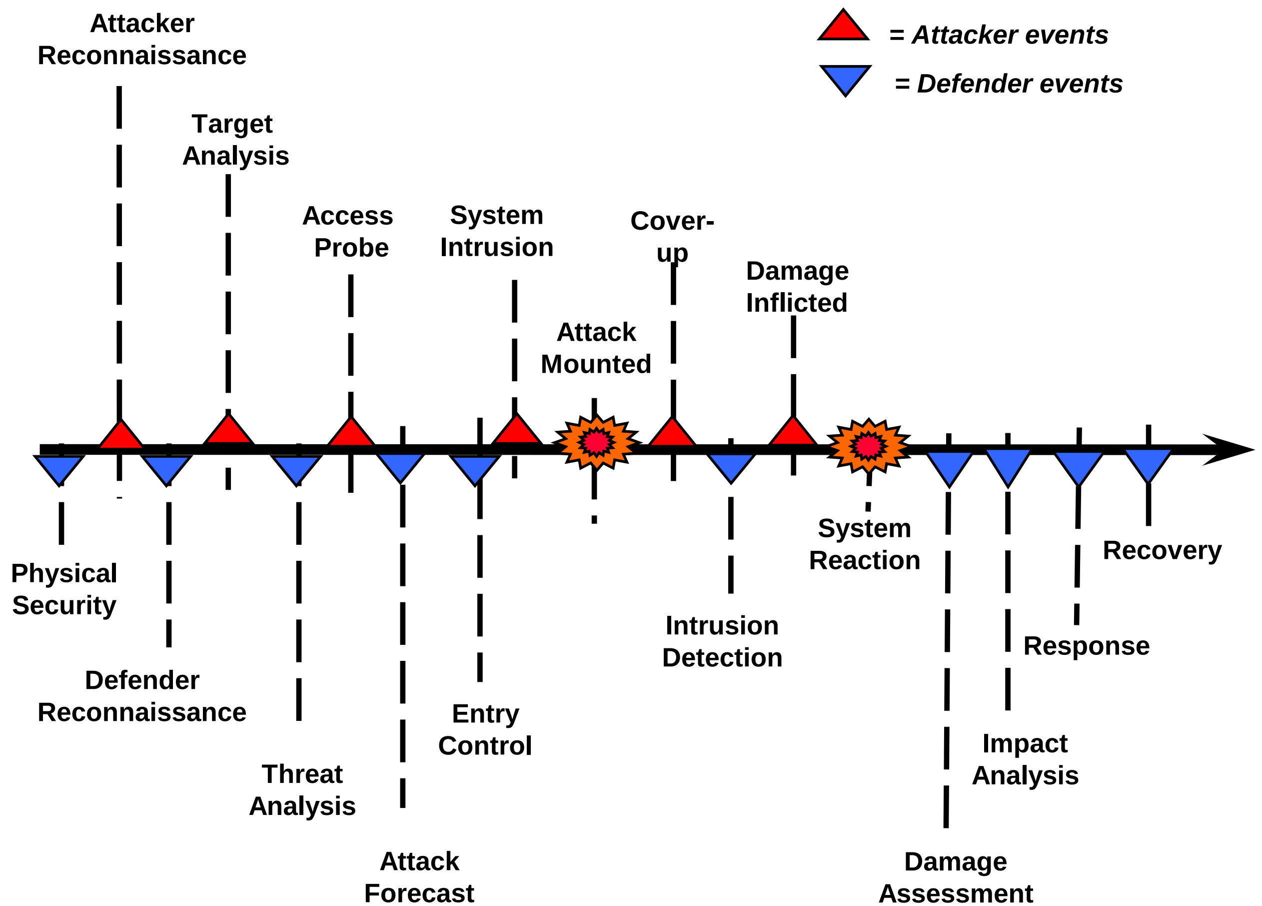
Then	Now
Computer nerd	Determined, funded adversary
Thrill seeking	Profit or political gain
Illegal but benign	Criminal intent

The major threat vectors



Anatomy of an Incident

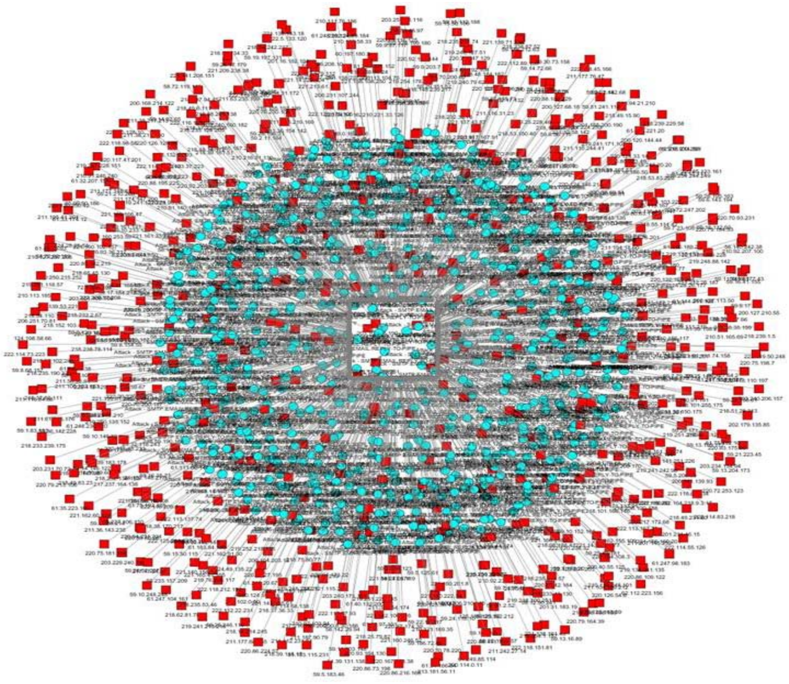
NORTHROP GRUMMAN



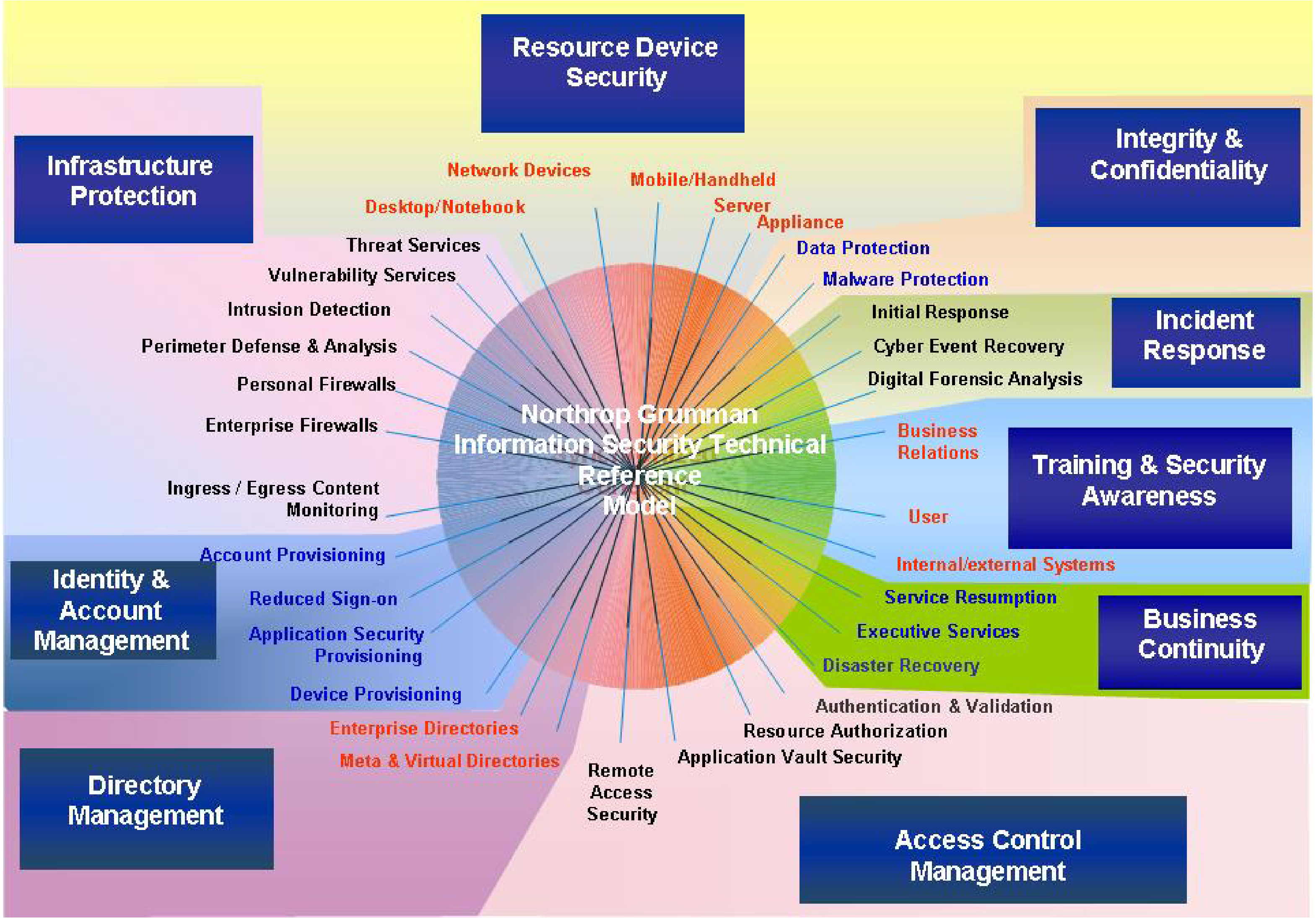
- Course look at the timeline of an attack showing more the reactionary state of defense
- How does this correlate to the Threat
- Issue becomes how to defend effectively at all points from a data view

Current Perimeter Centric Architecture

- Large flat network that is at best two-dimensional
- Protection mechanisms exist at the border where string authentication required
- Questionable configuration consistency - Data is scattered with multiple versions and copies
- International situation confusing due to information propagation and cross border data issues
- Protection uses risk as justification for investment



Security Architecture Components



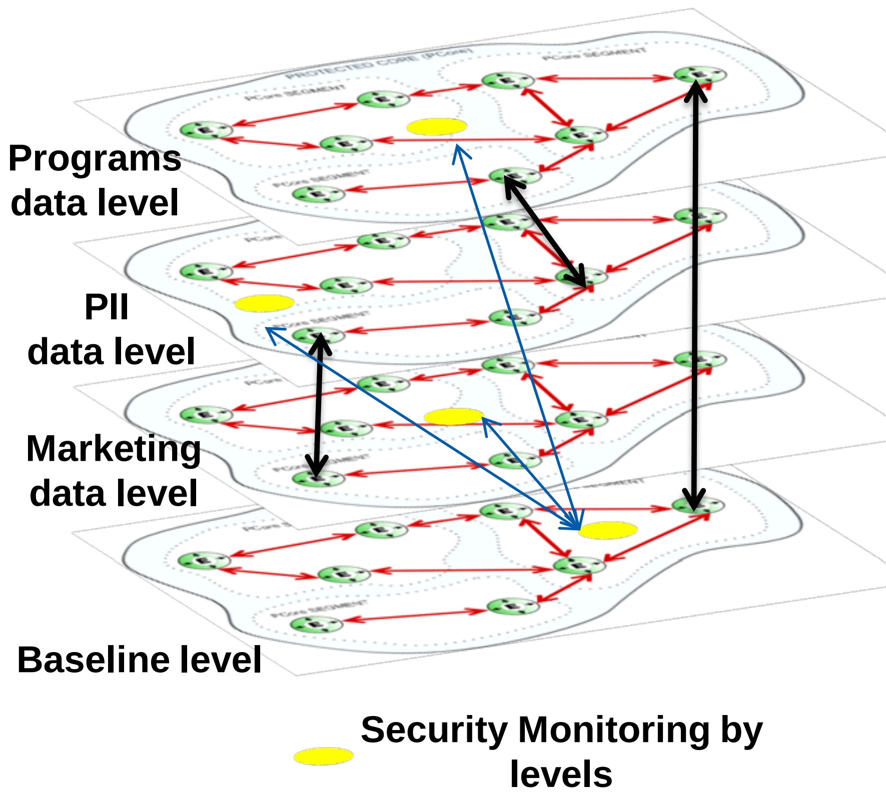
Technical reference model provides a "completeness" check

Security Architecture Description

- Everything being under the same roof gives latitude and allows for some “security truths” to be assumed
- Backup and contingency concepts have to be fully developed.
- Concept of hierarchical/federated security
  - Linkages between segments can be “understood” as part of the architecture components
  - Follow the precepts of minimal essential information: only the data that is absolutely required
  - Communications are encrypted and well defined
- Layered security reporting/auditing
  - Can establish a multi-tier approach to reducing data load, pre-process at edge points, aggregate at Core level
- Mini-management functions (Core and segment level)
- Credentialing
  - Well defined approach to vetting individuals and network components
  - Have functions for add/delete/modify for all actors
  - Credentials never passed in the clear, always encrypted
  - Federate the identity management and use certificates

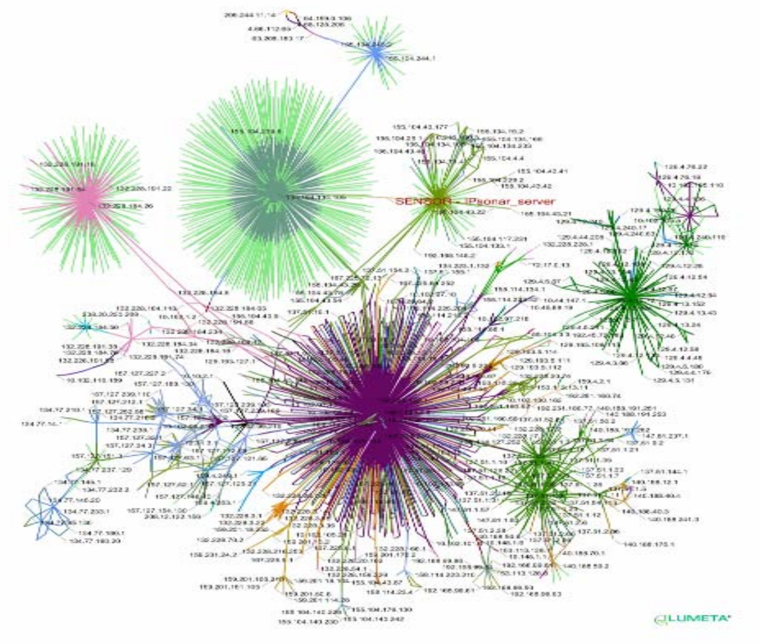
Notional Architecture by Function

- Un-flatten the network
  - Opportunity with IPv6
  - Focuses security monitoring
  - Example here is via data
- Access
  - Tightly controlled
  - Can set in the paths
  - “Have to be in the right lobby to get the right door”
- Security Monitoring and Control
  - Local, allowing for disconnect if necessary
  - Reduction of information can begin at lower levels
  - Better ability to aggregate and react in real-time



Tracking information... the value of labeling

- Information tags/labels contain both attributes and policies
  - Data is labeled and tagged, therefore tracking throughout the system is straightforward
  - Cross border handling correlations can be easily done
- Indicates storage areas and network travel paths
- Identification analyzes duplication, confirming users roles and information use patterns
- Visually depicts the enterprise network and data types
- Can correlate who is using what, where it is being used, and how it is used.



Color coded view of the network and the information within

Variety in Authentication

Token	13th Century	Today
Name	William	Wmcleve2
Location	William of York	111.17.20.2
Hard (Provisioned) Possession	Medallion, sword, crest	Provisioned laptop, key fob, BlackBerry
Soft Possession	Password	Password
Appearance	Hair/eye/height	Facial scan
Knowledge	Secret	Secret
Biometric	Scar	Retina, fingerprint
Certification (3rd party verification)	Letter from king, with seal	Medium assurance soft PKI certificate

Authentication – Single factors

NORTHROP GRUMMAN

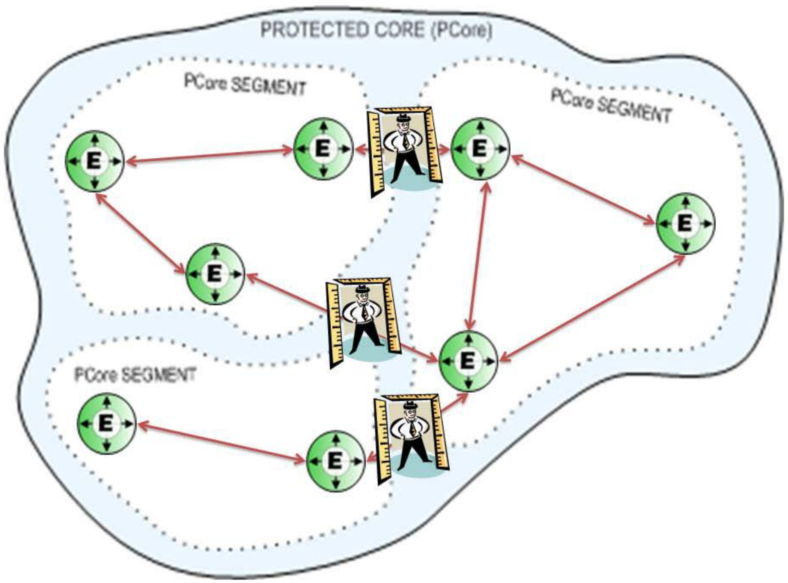
Method/Artifact	Assurance
Self-registered User ID/Shared Password/User Id	Little or no trust
Biometric: no control on biometric initialization.	Little or no trust
IP Address	Little or no trust
Private Password associated with User ID	Low Trust
Biometric: Trusted initialization local verification	Low Trust
Site Key	Low Trust
Biometric: Trusted initialization + central verification	Medium Trust
Trusted Medium assurance SW/ x.509 certificate	Medium Trust
One-time Password, Soft token	Medium Trust
RSA Hard token/PIN	Strong Trust
Medium Assurance HW/x.509	Strong Trust

Aggregation Results – Strength and Resilience

Aggregated Authentication Artifacts (examples)
Active Directory Id and Password (AD/PW)
Site key + AD/PW
Enterprise medium assurance certificate + AD/PW
(RSA) One Time Password + AD/PW
Medium assurance certificate + pin +AD/PW
Trusted medium assurance certificate + verified biometric + AD/PW
Properly provisioned laptop + fingerprint + physical access

Implementing authentication in a PC environment

- Different segments can use different approaches
  - Have to know which credential is valid and from where in the architecture can it be invoked
  - Wide latitude of which piece of information ties to which credential
- Looking for 2 things:
  - Authentication Consistency – All facets of the data seem to match (Joe is on vacation, not in the plant, not on the interior network, on the portal)
  - Authentication Inconsistency – Something is out of line (Joe is on vacation, not in the plant, on the interior network, not on the portal)



"We must look for consistency. Where there is want of it we must suspect deception."

http://www.sherylfranklin.com/sh-gillette.html

Provisioning: an Authentication Artifact

- Requires a vetted and certified trusted provisioning process
  - User is vetted
  - Provided with laptop serial #aa-tt, that is fingerprint enabled
  - Certified/trusted examiner loads laptop TPM with user's fingerprint and locks it in
  - User plugs into internal corporate network, swipes finger, is authentication……no need for user id/password
- Why does this work?
  - User was properly vetted by organization
  - Laptop was specifically assigned to user
  - Laptop only accessible by user and selected admins
  - Fingerprint properly loaded and vetted serves as combination user id/password but is stronger
    - Laptop is something you have and was specifically assigned to you (so it is something you have and to some degree something you know and are)
    - Fingerprint is something you are

CAI Enhancements

NORTHROP GRUMMAN

- Can fully federate identities, ensuring current status are maintained
- Authentication approaches allow greater flexibility from the usual User ID/Password/Token/Card
- With federating the security monitoring functions, can be less reactive
- IPv6 offers greater control potentials

Summary

- Increased the bad guy expose time, have forced a lot of running the hallways to find the right door
- Attack sensed in one area allows for blocking that subnet stemming the infection
- Attacks learned in one segment are lessons to all segments
- Attack surface is not smooth, no guarantee for the attacker that entry in one area ensures freedom to other areas
- Adding/subtracting segments based on enterprise functionality
- Can monitor internal use/mis-use much better.

Assessment of the Challenges

NORTHROP GRUMMAN

- This is large undertaking but manageable (leverage IPv6)
- Requires re-thinking about architectures
- Technologies will enforce change
- Will result in new policies, directives, and SOP
- Data identification and labeling becoming SOP
- Investment has positive Enterprise impacts

2

Legend **People** **Process** **Technology**

NORTHROP GRUMMAN

NDIA 6TH ANNUAL DISRUPTIVE TECHNOLOGIES CONFERENCE

Washington DC
October 14 – 15, 2009

… simply better protection!

Title: NEW PACKAGING AS A CLUTTER REDUCTION METHOD

Keith Donaldson

Director of Research & Development
Intercept Technology Group

Joe Spitz

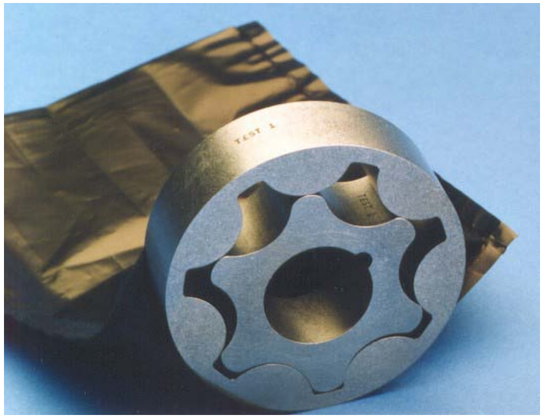
Sales & Marketing
Intercept Technology Group

www.LibertyPackaging.com

www.StaticIntercept.com

Clutter comes in many forms

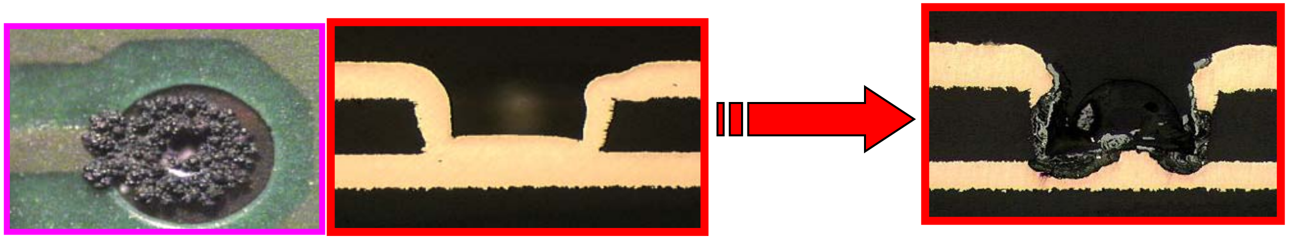
How to get it safely across the ocean?



How to protect without oil?

How to locate something packed in a barrier material?

Obsolete but not driven?



How to prevent failure in a circuit in traditional ESD packaging after 6 weeks in India…

Clutter

- Caused by dis-organizational issues
- Caused by excessive packaging
- Caused by the use of non-recyclable packaging
- Caused by the use of packaging that cannot be opened and re-sealed in the field, resulting in waste, in-efficiencies and creation of lost parts and debris (scrap)
- Caused by obsolete parts and field failures
- Caused by thick layers of regulations that have not allowed for flexibility, change or streamlining

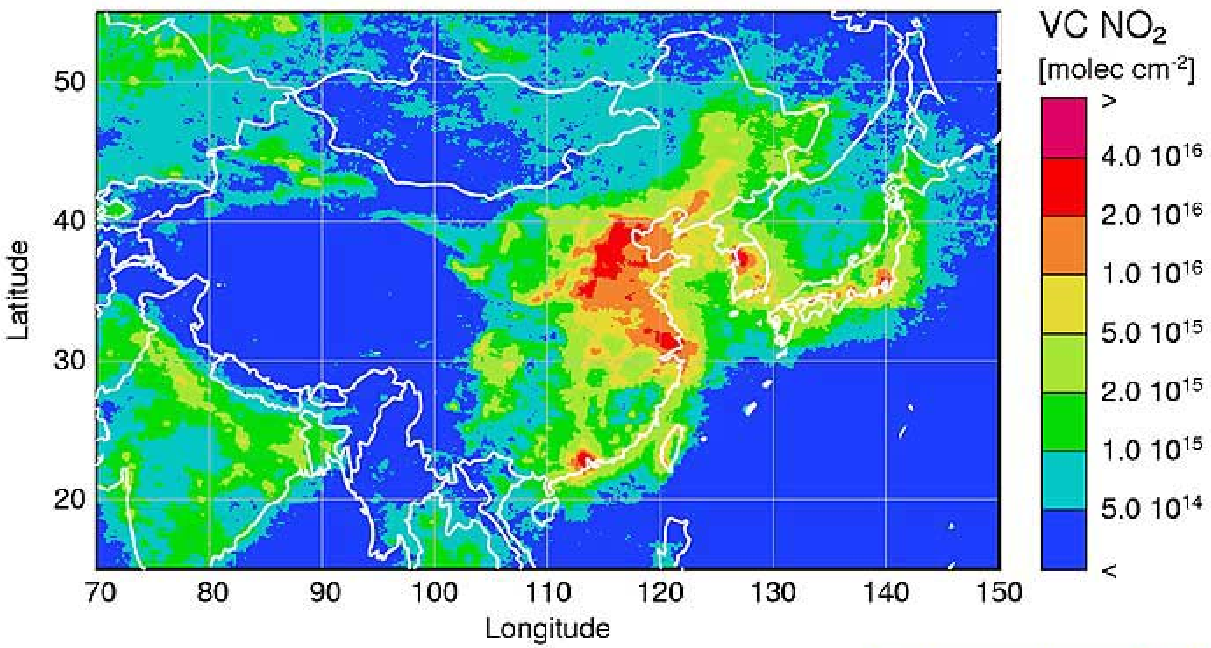
Packaging and De-Cluttering

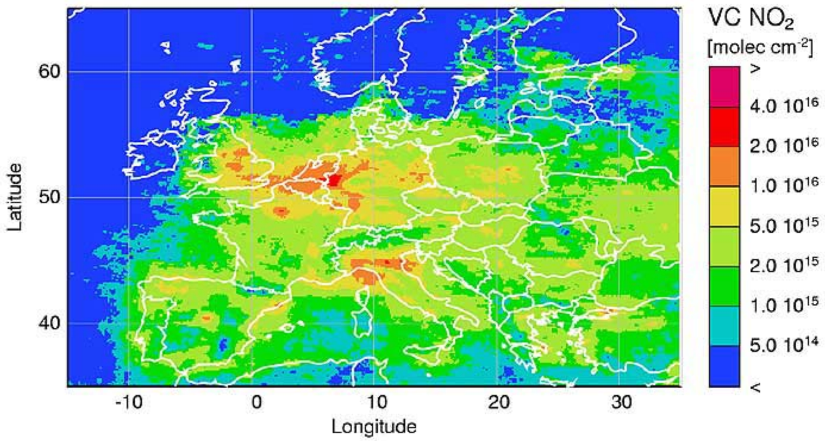
- Environmental Concerns
- Minimization of Packaging
- Effectiveness of Packaging
- Impact of RoHS and other legislation
  - Restriction of Hazardous Substances (RoHS)
  - TRGS Legislation in Germany / Europe
- Need for more robust Packaging
  - i.e. Active barriers instead of passive ones
- Need to look for new technologies, new developments

Environmental Impacts

- 3 R's
  - Reduce / Re-Use / Re-Cycle
- Carbon Footprint
- RoHS and environmental legislation in Europe
- Increase in air pollution worldwide putting more stress on products, many already compromised by RoHS restrictions
- Recycability versus landfills
  - Equally important is to develop / push re-usable packaging to reduce overall packaging needs

An aerial view of the Worsening Worldwide Corrosion Issue





Global Economy - Atmosphere

"If one visits Mount Hood in Oregon one can see that the snow on the side of the mountain facing China has grey shade while the east side is bright white"
James Brenzel
The Economists
Sept 30th, 2006


"All the News That's Fit to Print"

The New Yo

VOL. CLV . No. 53,607 — NEW YORK, SUNDAY, JUN

Pollution From Chinese Coal Casts Shadow Around Globe

By KEITH BRADSHER and DAVID BARBOZA

THE ENERGY CHALLENGE
The Cost of Coal

HANJING, China — One of China's lesser-known exports is a dangerous brew of soot, toxic chemicals and climate-changing gases from the smokestacks of coal-burning power plants.

In early April, a dense cloud of pollutants over Northern China sailed to nearby Seoul, sweeping along dust and desert sand before wafting across the Pacific. An American satellite spotted the cloud as it crossed the West Coast.

Researchers in California, Oregon and Washington noticed specks of sulfur compounds, carbon and other byproducts of coal combustion coating the silvery surfaces of their mountaintop detectors. These microscopic particles can work their way deep into the lungs, contributing to respiratory damage, heart disease and cancer.

Filters near Lake Tahoe in the mountains of eastern California "are the darkest that we've seen" outside smoggy urban areas, said Steven S. Cliff, an atmospheric scientist at the University of California at Davis.

Unless China finds a way to clean up its coal plants and the thousands of factories that burn coal, pollution will soar both at home and abroad. The increase in global-warming gases from China's coal use will probably exceed that for all industrialized countries combined over the next 25 years, surpassing by five times the reduction in such emissions that the Kyoto Protocol seeks.

The sulfur dioxide produced in coal combustion poses an immediate threat to the health of China's citizens, contributing to about 400,000 premature deaths a year. It also causes acid rain that poisons lakes, rivers, forests and crops.

The sulfur pollution is so pervasive as to have an extraordinary side effect that is helping the rest of the world, but only temporarily: It actually slows global warming. The tiny, airborne particles deflect the sun's hot rays back into space.

But the cooling effect from sulfur is short-lived. By contrast, the carbon dioxide emanating from Chinese coal plants will last for decades, with a cumulative warming effect that will eventually overwhelm the cooling from sulfur and deliver another large kick to global warming, climate scientists say. A warmer climate

Continued on Page 12


NASA - Sea of Japan


Shanghai, China
After a cleansing rain storm


Shanghai, China
Typical day


Brazil


South Korea

Industrial Economies make it difficult to ship or store electronics or equipment

A better alternative?

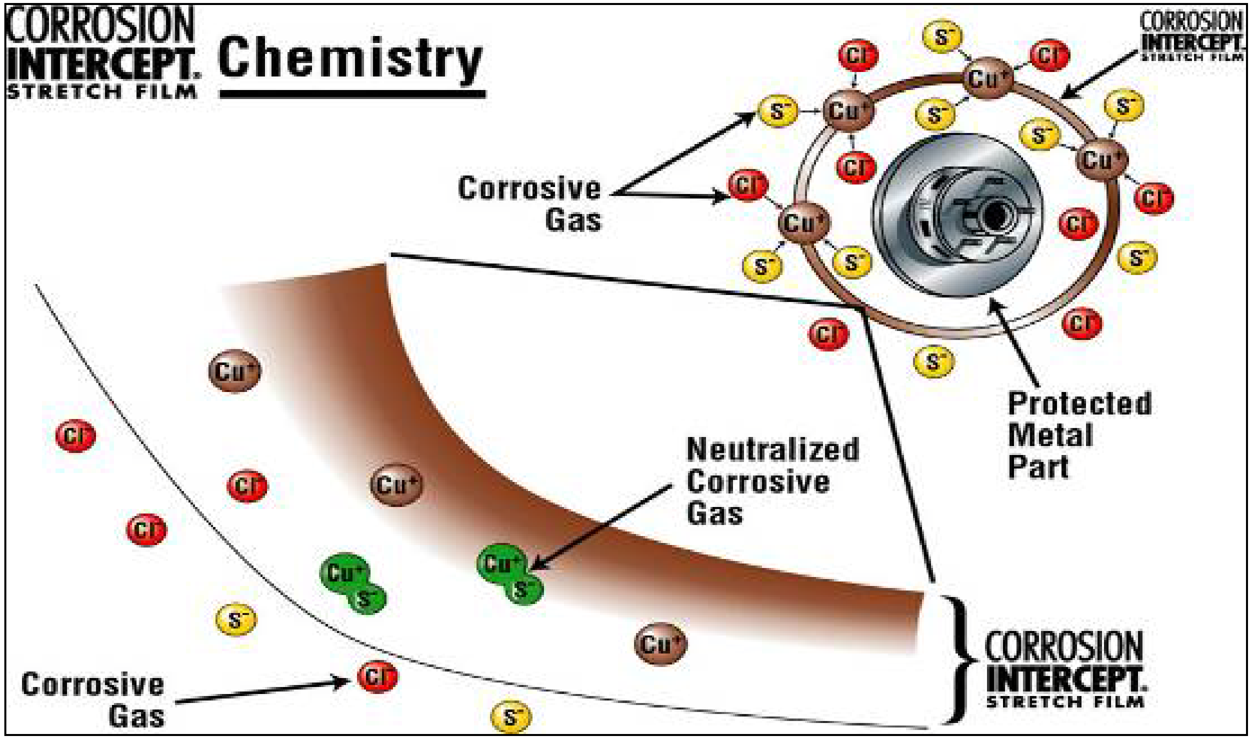
Environmental Impacts

- Reactive versus Passive Barrier
  - We need to demand more from our packaging
  - Current Mil B-131 bags are passive barriers
  - Changes in packaging, such as the Intercept Technology, provide reactive barriers, actively providing protection
  - Intercept Technology goes even farther, providing more than a 50% reduction in carbon footprint over a mil 131 bag
  - Additionally, Mil-131 bags are not recyclable, leading to increased landfill usage and more clutter in military settings

INTERCEPT

INTERCEPT TECHNOLOGY™

INTERCEPT was developed and patented by Lucent Technologies and Bell Laboratories in 1987. Highly surface area copper particles are permanently reacted into a plastic matrix and then allowed to react with all corrosive gases as they try to penetrate the film or bag. The Technology was designed to protect all materials under all environmental conditions equally. The material is volatile free so no increase in VOC loading and is not a VCI.



US Army TACOM (Tank Command) EVALUATION OF INTERCEPT BARRIER MATERIAL FOR MILITARY PACKAGING

SALT-FOG Test Data Comparison

<<<<< Days of protection against corrosion >>>>>>>

Metal coupon	Intercept Poly 4-mil	VCI Poly 4-mil	MIL-PRF-131 Foil / Poly 5-mil
Steel	102	28	62
Aluminum	130	59	91
Brass	130	28	91
Zinc	97	59	77

Sam Sakar - 8th Annual Government/Industry Shelf-life Symposium, October 29-31, 2002
Kansas City, Missouri

Re-Usability

- Equally, if not more important than recycling is to be able to reuse a packaging material and/or be able to re-seal it (close it) in the field.
  - Foil bags (mil 131) require RH below 37%, so they cannot be re-sealed easily in the field, it would require additional desiccant and vacuum sealing equipment
  - Also, cannot read RF signals through foil
  - Intercept can easily be re-taped in the field
- Re-using reduces the overall packaging material, while providing the ability to decrease clutter.
  - Intercept is designed for 5 to 10 years or more of protection / easily allowing for re-use applications

Examples of Re-Use

Small components to large dunnage systems can be re-used, reducing cost and clutter

Fuel injectors – small vacuum formed tray that took a corrosion critical part from 300% inspection to 200% and one way packaging to over 3 years use with no failures

Engine block bags for shipments between continents and storage

Examples of Re-Use

A NIPHLE Packaging Award winner

Intercept was used to line the crates to ship the armored plated cabs to the Middle East, the same crate was then used to return the old, non-plated cabs.

No Rust / No Failures

Reduce

- The ultimate goal of packaging is to reduce the amount of it, or to reduce the amount of additional materials required to get our products / materials safely to their destination. Advanced shrink films can allow a reduction in crating required.

Effective shrinkwrap allowing safe deck top shipping

Old Method

Gerotor

Spray Oil Coat

Apply wax Cheesecloth

Put in PE Bag

Put in Foil Bag

Vacuum Seal

Box and Store / Ship

5 Processes (Steps)
Air Handling Requirement
4 Materials
Total Pack Time - **25 Minutes**

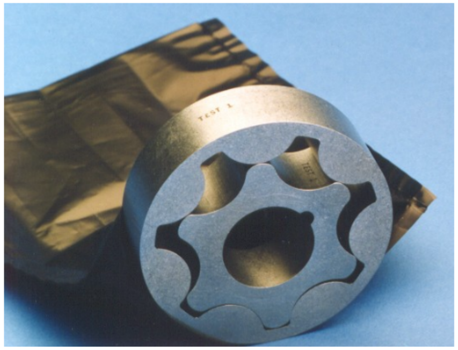
Intercept Method

Gerotor

Place in Static Intercept Zipper Closure Bag

Box and Store / Ship

1 Process Step (no air handling concern)
1 Material (reduced inventory and cost)
Total Pack Time - **5 Seconds**
No Rejections



Over 120,000

Parts packed

“0” Rejects

Weaving Machine traveling between Germany and Russia – sat outside for 3 months after 8 – 10 week sea shipment. Arrived in perfect condition.

Quick Pack Method:

-Place 4 mil oversize bottom sheet on pallet
-Place equipment on bottom sheet
-Place pre-made bag over equipment
-Bring up excess bottom sheet and securely tape around the whole item – overlap the bottom sheet and bag by 6 inches
-Can evacuate for better performance
-May add desiccant if going overseas

Intercept Technology™

1. Green Packaging – Recyclable / Re-usable / Sustainable
2. Permanent ESD protection – long term Corrosion protection
3. No contamination – no outgassing (ideal for aerospace)
4. Ease of use
5. Proven effective
6. Approved and used by key companies and militaries worldwide
7. Easier and more effective than foil packaging
8. RFID transparent – an active barrier that can have RFID transmission
9. Same packaging can be used for short term or long term storage
10. Flexibility and availability
11. Protects against Bio-Corrosion

Thank you for your time

Liberty Packaging Company

A member of the Intercept Technology™ Group

www.LibertyPackaging.com

www.StaticIntercept.com

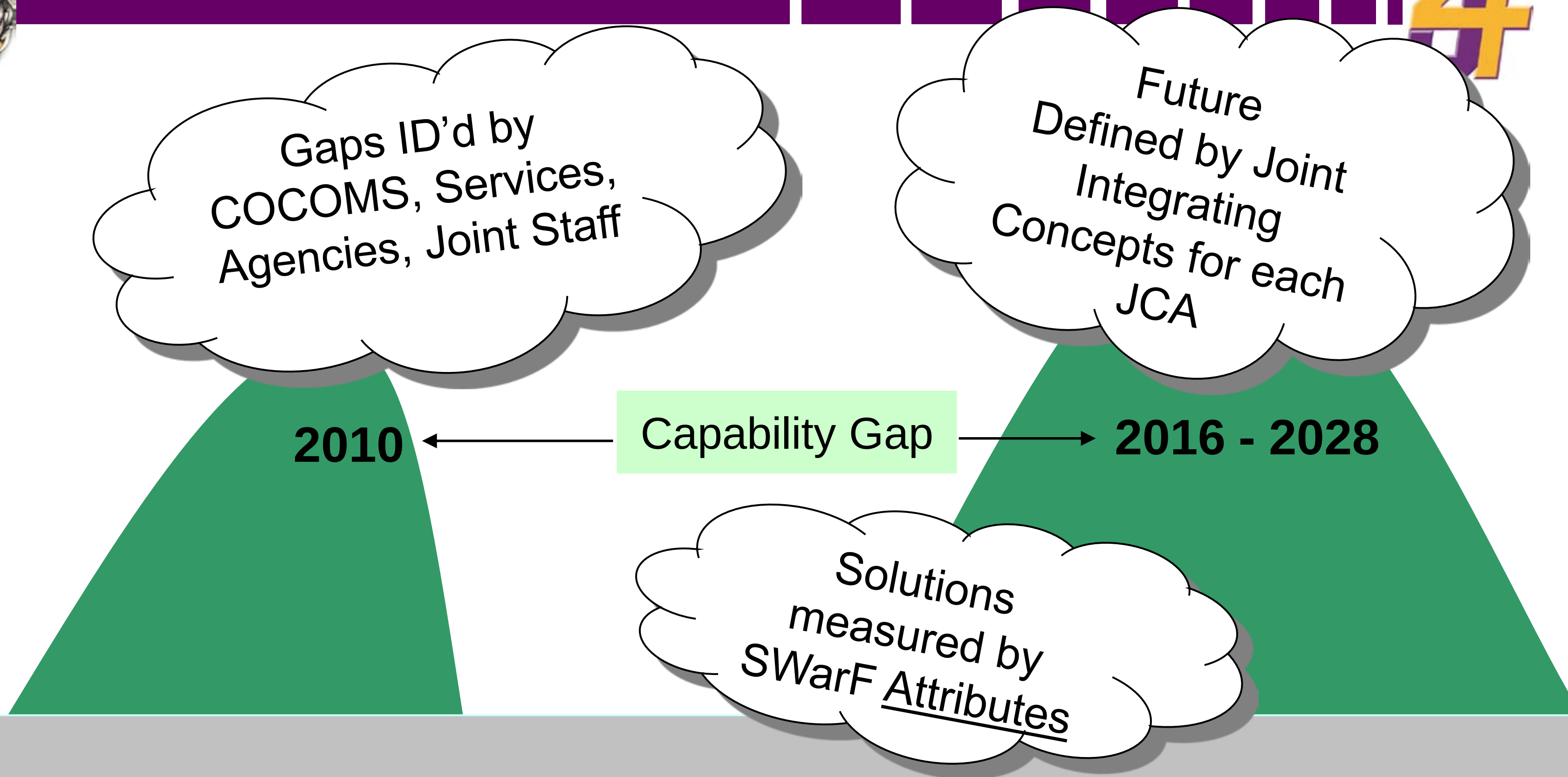
NDIA Disruptive Technologies Conference Logistics Gaps

Lt Col Lisa Hess
Joint Staff (J-4)
Logistics Functional Capabilities Board

Purpose

To outline Logistics capabilities and potential avenues for S&T focus

Logistics Capability Landscape



Joint Capability Areas

Supply – Maintain – Contracting Support – Engineering
Deployment and Distribution – Logistic Services – Installation Support

Deployment and Distribution

- Move the Force
- Sustain the Force
- Operate the Joint Deployment Distribution Enterprise (JDDE)

<u>Attributes</u>
Visibility
Reliability
Velocity
Precision
Capacity

<u>Potential Areas of Interest</u>
Intra-Theater Distribution
Fuel and Ammo Mobility
Operational C2
Seabasing
Cyber Protection
Forced Entry
Agile Logistics
CBRNE Survivable

Deployment and Distribution (Cont'd)

- Move the Force
- Sustain the Force
- Operate the Joint Deployment Distribution Enterprise (JDDE)

<u>Attributes</u>
Visibility
Reliability
Velocity
Precision
Capacity

<u>Potential Areas of Interest</u>
Containerization
Sustainment
Inter-Theater Airlift
Aerial Refueling
Strategic Sealift
Distribution Networks
Unmanned Logistics Delivery Systems
Autonomic Logistics
Energy Reduction

Supply

- Manage Supplies & Equipment
- Inventory Management
- Manage Supplier Networks

<u>Attributes</u>
Responsiveness
Sustainability
Flexibility
Survivability
Attainability
Economy
Simplicity

<u>Potential Areas of Interest</u>
Prepositioning

Maintain

- Inspect
- Test
- Service
- Repair
- Rebuild
- Calibration

<u>Attributes</u>
Sustainability
Responsiveness
Attainability
Flexibility
Economy
Survivability
Simplicity

<u>Potential Areas of Interest</u>
Predictive Maintenance
Remote Monitoring

Logistic Services

- Food Services
- Water and Ice Service
- Basecamp Services
- Hygiene Services

<u>Attributes</u>
Responsiveness
Attainability
Sustainability
Flexibility
Economy
Survivability
Simplicity

<u>Potential Areas of Interest</u>
Water Packaging
BARE Base Set Generator
Modular Services
Mobile Food Services
Mobile Mortuary Affairs
Expeditionary Basing

Operational Contract Support

- Contract Support Integration

- Contractor Management

<u>Attributes</u>
Responsiveness
Attainability
Flexibility
Survivability
Sustainability
Simplicity
Economy

<u>Potential Areas of Interest</u>
Process Management

Engineering

- Combat Engineering
- General Engineering
- Geospatial Engineering

<u>Attributes</u>
Effective
Expeditionary
Agile/Tailorable
Networked
Integrated
Precise
Enduring/Persistence

<u>Potential Areas of Interest</u>
Airfield Damage Repair
Well Drilling

Installation Support

- Real Property Life Cycle Management
- Installation Services

Attributes
Responsiveness
Sustainability
Flexibility
Survivability
Attainability
Economy
Simplicity

Potential Areas of Interest
Portable Airfield Lighting
Base Support

Discussion

NDIA Disruptive Technologies Conference

Supporting the Warfighter: Building a Robust, Joint Triad Network

COL Bill Hickman
Joint Staff J8 /
United States Joint Forces Command J8F

Command and Control Functional Capabilities Board

Purpose

Inform industry of Joint Command and Control (C2) Capability Gaps as industry develops future C2 solutions in support of the warfighter across the range of military operations

US Joint Forces Command (USJFCOM)

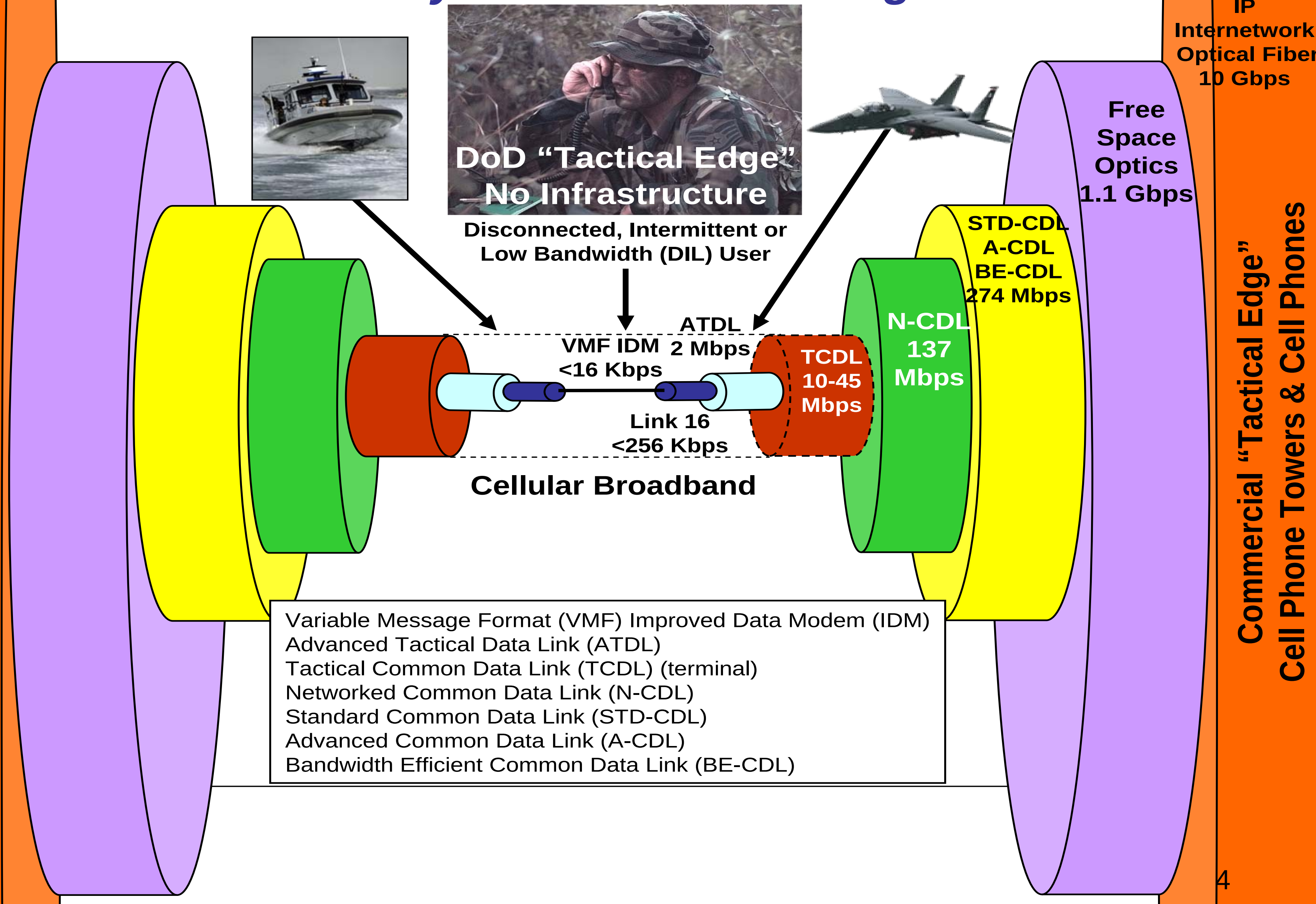
- C2 Capability Portfolio Manager -- Manage designated Joint C2 portfolio programs, systems, and capabilities across the whole spectrum of doctrine, organization, training, material, leadership and education, personnel, and facilities

- Delegated authority to manage & recommend approval to Joint Requirements Oversight Council (JROC) for Command and Control portfolio

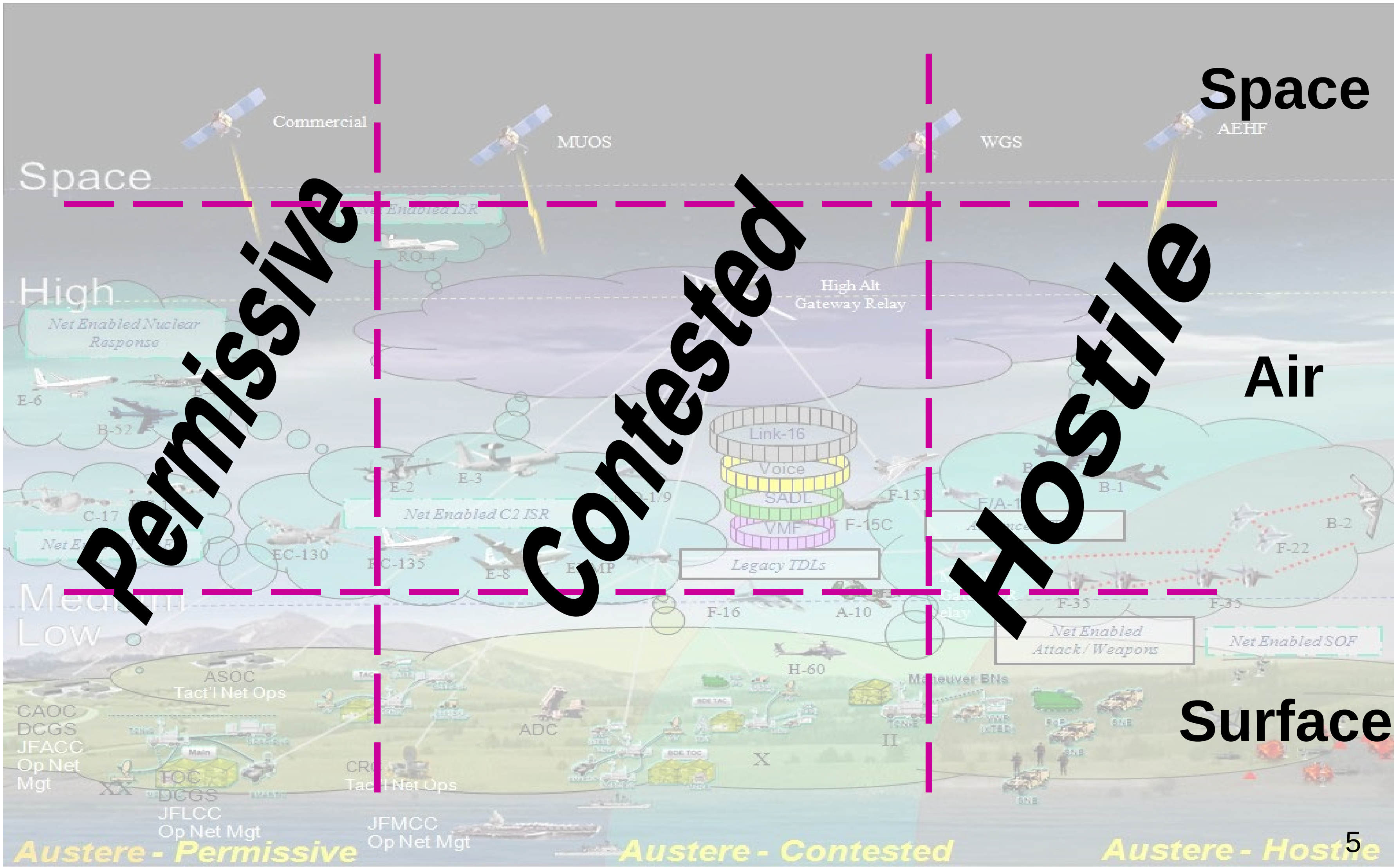
  - C2 JCB – Makes recommendations on JROC interest documents and assists JROC in carrying out its duties and CJCSI 3170.01G responsibilities

  - C2 FCB -- Integrates stakeholders views on C2 concept development, capabilities planning, and force development to ensure U.S. military can execute assigned missions

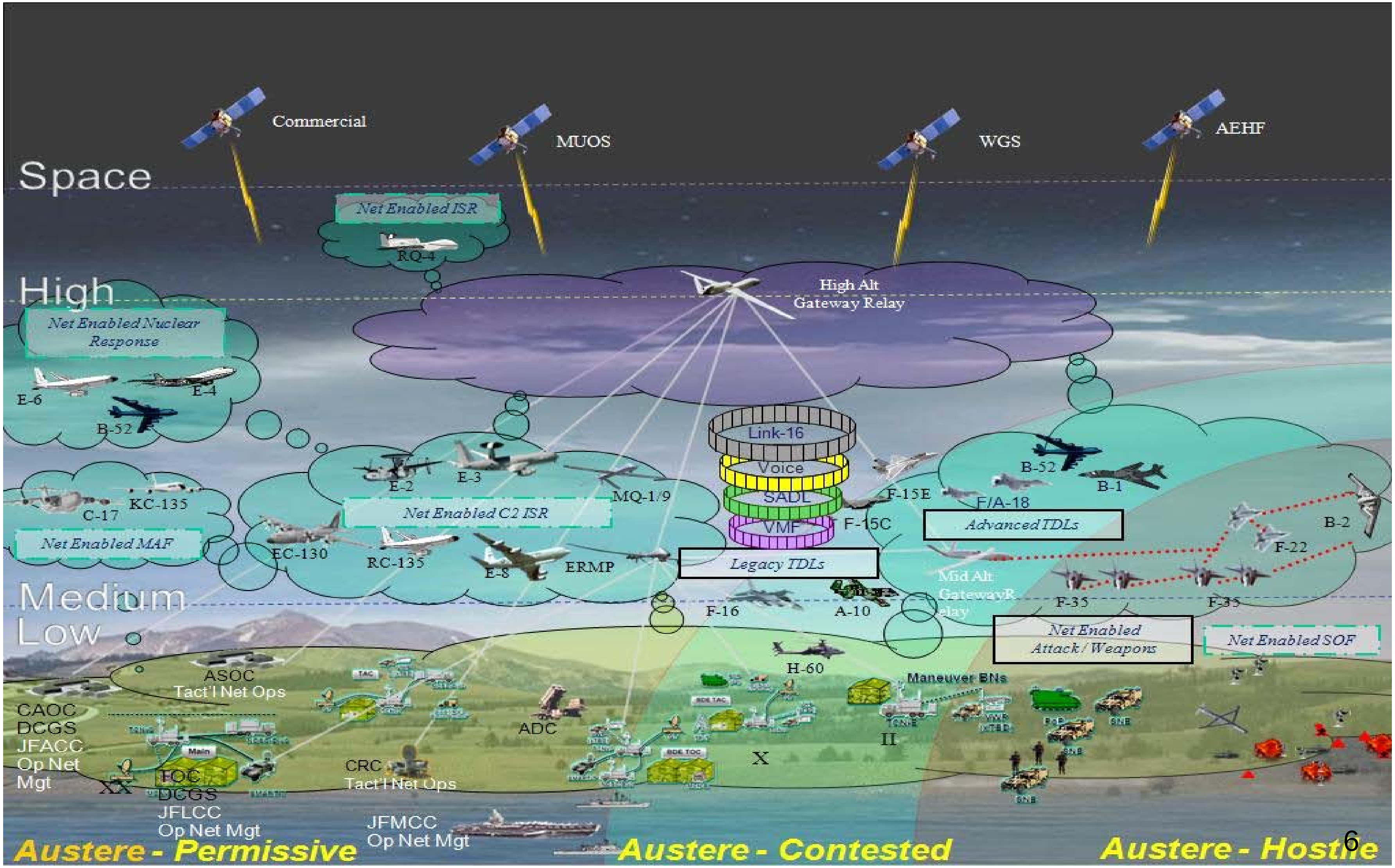
Commercial vs DoD "Tactical Edge"
The Physics of Net-Enabling



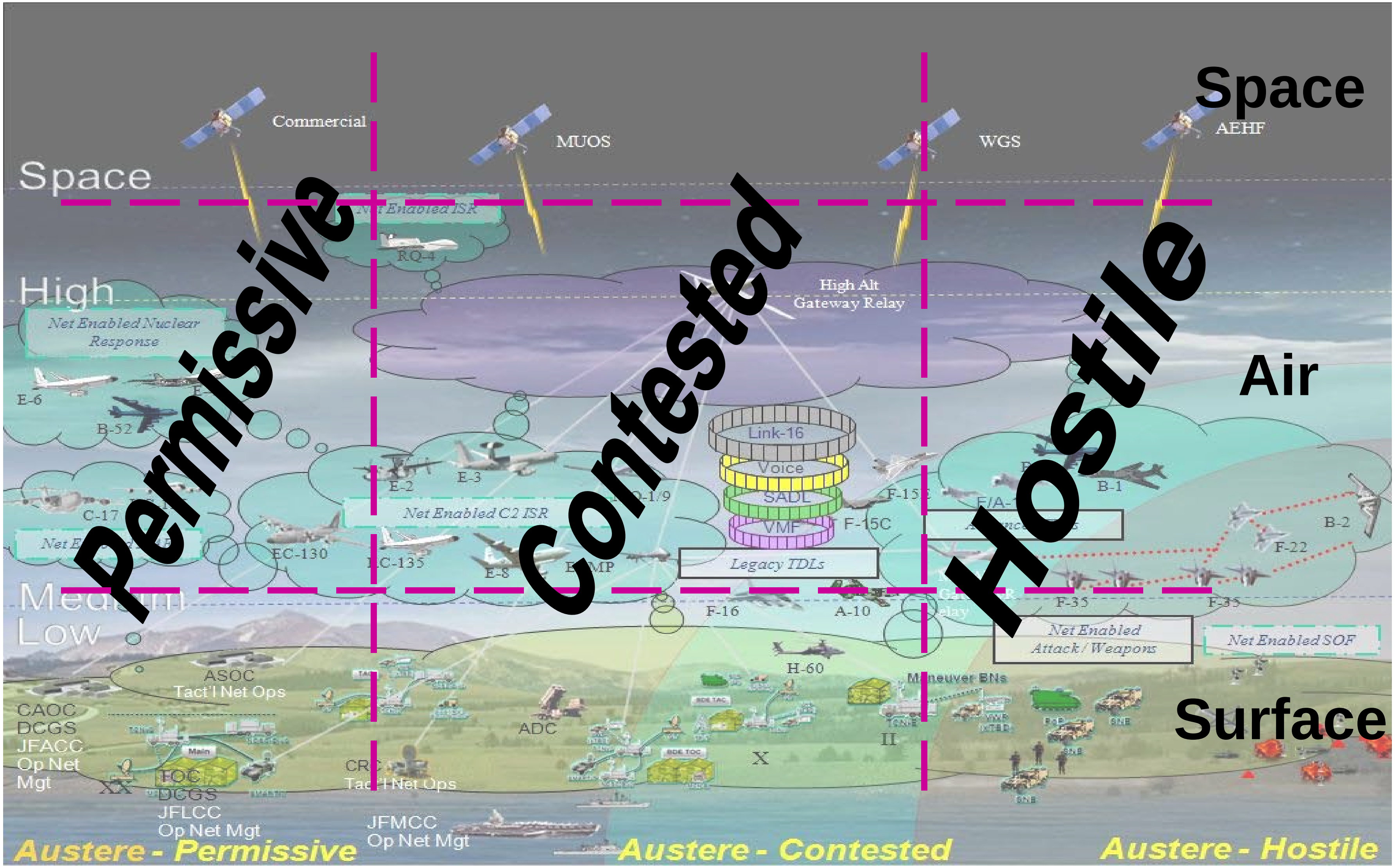
Leader Centric C2 ↔ Tactical Edge
Very Technical / Very Complex



Leader Centric C2 ↔ Tactical Edge
Very Technical / Very Complex



Leader Centric C2 ↔ Tactical Edge
Very Technical / Very Complex



Command and Control (C2) Capability Gaps & Challenges

Joint Space Communications Layer (CONOPS)

JSCL Provides persistent survivable assured beyond line of sight communications that facilitate C2 for all users including coalitions/allies across the range of military operations

- **Operational Challenges / GAPS**
  - **Global coverage and capacity when & where needed**
  - **Seamless communication**
  - **Integration into the Global Information Grid (GIG)**
  - **Survivability**

➢ **Interoperability with COCOMS, JTF, & Coalition Partners**

Joint Aerial Layer Network (ICD)

JALN Integrated with space and surface networks enables Leader Centric C2 and Battlespace Awareness in a net-enabled environment, enabling advanced warfighter information exchange capabilities across the range of military operations

- **JALN Capability GAPS**
  - **Connectivity**
  - **Capacity**
  - **Aerial Layer Network Management**
  - ➢ **Share Information and Data**

Command and Control On The Move (ICD)

C2OTM is the capability to maintain situational awareness and make timely and informed decisions while moving anywhere within the operational environment across the range of military operations

- **<u>C2OTM Capability GAPS</u>**
  - **Disconnected, Intermittent, Low Bandwidth Environment (DIL)**
  - **Common Interoperability Standards**
  - ➢ **Maintain & Share Situational Awareness**
  - ➢ **Accurate C2 to Subordinate Units & Mission Partners**
  - ➢ **Collaborative Planning**
  - ➢ **Shared Information with Mission Partners**

C2 Triad
Capability GAP Overview

- – Common Interoperability Standards
- – Global coverage and capacity when and where needed
- – Connectivity
- – Integration into Global Information Grid (GIG)
- – Survivable
- – Network Management

- ➢ Seamless communication ensuring accurate C2 to Subordinate Units and Mission Partners
- ➢ Shared Information/Data with COCOMS, JTF, and Coalition Partners
- ➢ Provide Collaborative Planning

Warfighter Tactical Edge

- **Very Technical, Very Complex**
- **Jointness is <u>Not</u> Natural**
- **Information Age Making it…**

  More Important and More Difficult
- **Need Processes for Collaboration / Consensus Building**
- **Need to Work Solutions Through Multiple Lanes With Partners**
  - Requirements
  - Acquisition
  - Programs
- **Need Technically Competent, Operationally Focused Assessment**

★ **Collaboration** ★ **Consensus Building** ★ **Compelling Logic** ★

Questions and Discussion

COL Bill Hickman, C2 FCB Lead

NIPRNet -- **william.hickman@js.pentagon.mil**

SIPRNet -- **william.hickman@js.smil.mil**

703-692-8006 (DSN: 222)

NDIA 6th Annual
Disruptive Technologies Conference

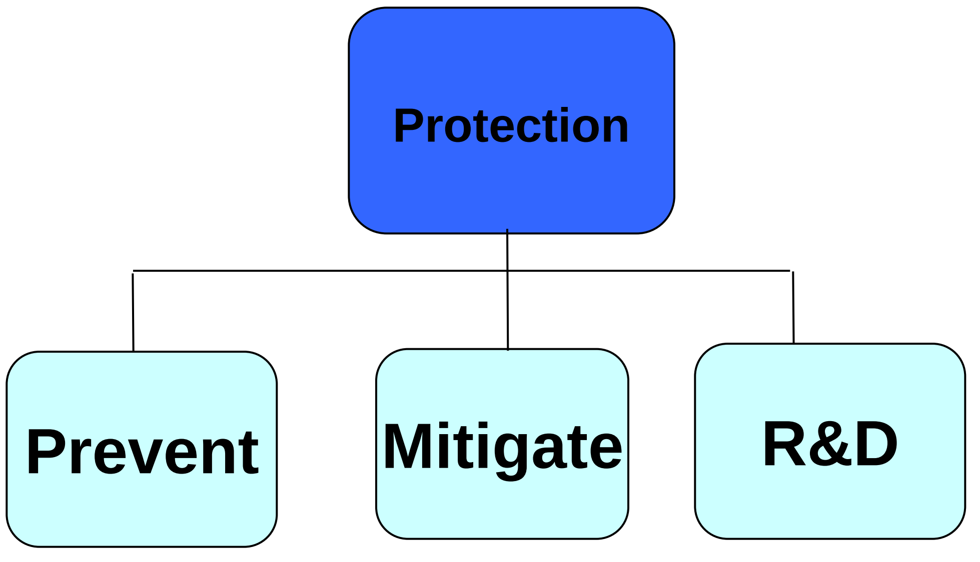
Protection Operational Capabilities

Steve Inada
DDFP Support Division
Joint Staff/J8
Protection Functional Capabilities Board
(703) 571-3046 (DSN 671)
October 15, 2008

Purpose and Agenda

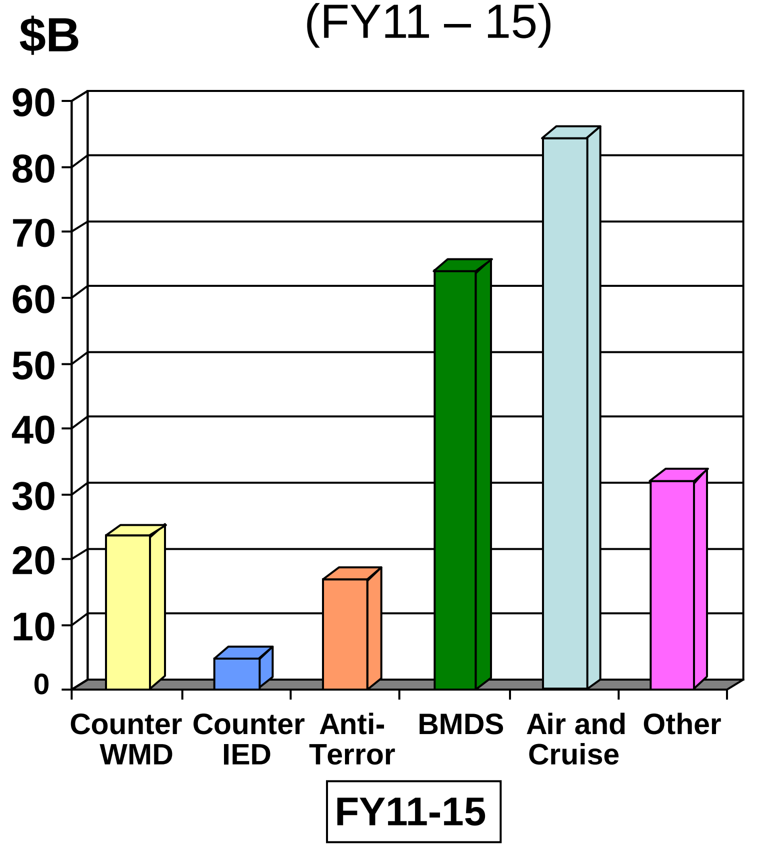
- Purpose: To provide an overview of protection portfolio and associated desired operational capabilities
- Background of Protection Portfolio
- Protection Joint Capability Areas
- Major Portfolio Inputs
- Portfolio Portfolios and JCAs Linkages
- Capability Goal and Gap Influences
- Goals and Attributes
- Desired Operational Capabilities

Protection DoD Portfolio
Background



Cross Cutting Protection Capability Mission Areas

988 programs
investment about $267B
(FY11 – 15)



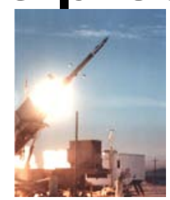
Protection Joint Capability Area

Protection is defined as "the ability to prevent/mitigate the adverse effects of attacks on personnel and physical assets of the U.S., its allies, and its friends"

- **Prevent – The ability to neutralize an imminent attack or defeat attacks on personnel (combatant/non-combatant) and physical assets.**
  - **Prevent Kinetic Attack** – The ability to defeat attacks being delivered by systems which rely upon physical momentum.
  - **Prevent Non-kinetic Attack** – The ability to defeat attacks being delivered by systems which do not rely upon physical momentum.
- **Mitigate – The ability to minimize the effects and manage the consequence of attacks (and designated emergencies on personnel and physical assets.**
  - **Mitigate Lethal Effects** – The ability to minimize the effects of attacks or designated emergencies which have the potential to kill personnel and destroy physical assets.
  - **Mitigate Non-lethal Effects** – The ability to minimize the effects of attacks or designated emergencies which do not have the potential to kill personnel and destroy physical assets.
- **Research and Development – The ability to conduct fundamental research, science, technology, development and experimentation important to all Departmental capabilities and operations** (Basic, Applied, Advanced Technology Development)

Protection Portfolios

- **Air and Missile Defense (including the protection of U.S. space systems & capabilities)**




- **Combating WMD (including U.S. nuclear weapons security, consequence management of WMD attacks and natural disasters, and defense crisis management)**

- **Protection (including defense against IEDs and other kinetic attack means, and defense critical infrastructure protection)**

Protection FCB has three major sub-portfolios

Protection Portfolios and JCA Linkages

Air & Missile Defense

- **Active defense against air & missile attacks** (P & R/D)
- **Active and passive defenses of U.S. space systems and capabilities** (P, M, R&D)

Note: These activities are mapped to Force Protection's Tier 2 JCAs: Prevent (P), Mitigate (M) and R&D.

Combating WMD

- **Protection of U.S. forces from the impact of WMD attacks** (M, R&D)
- **Maintenance of control over WMD and related/precursor materials** (M, R&D)
- **Response capabilities to manage and mitigate the consequences of WMD attacks and of man-made or natural disasters** (M, R&D)
- **Prevention of WMD proliferation** (P, R&D)
- **Defense crisis management** (M, R&D)

Protection

- **Detection and defeat of IEDs at the point of attack** (P, R&D)
- **Active and passive defenses of U.S. forces, facilities, and equipment against attacks by IEDs and other kinetic means** (P, M, R&D)
- **Active and passive defenses to protect DoD critical infrastructure** (P, M, R&D)
- **U.S. nuclear weapons security** (P, R&D)

Major Portfolio Goal and Gap Influences

STRATEGIC GOALS AND OBJECTIVES

GDF/NMS/QDR
- Balanced Portfolio
- Protect against current and future threats
- Prevent proliferation of WMD
- Mitigate by improving crisis management

WARFIGHTER JOINT REQUIREMENTS

SWarF/FP FCB/JCIDS
- COCOM IPLs
- COCOM STIPLs, JCTDs
- Warfighter Challenges
- JUONS, DCRs
- CONOPs
- Joint Combat Capability Assessments

OPERATIONAL CONSIDERATIONS

- **Synchronizing:**
  - Requirements
  - Programming
  - Acquisition
- **Early/Rapid Technology Development**
- **Fielding and Sustaining Capability**

Capability Goals

- Capability Goals

  - Goal of Protection is to execute layered comprehensive and layered protection of the United States and friendly nation personnel and assets, both at home and abroad. Further, Protection seeks to provide commanders and warfighters with the ability to detect, deter, defeat, and/or mitigate attacks on both combatant and noncombatant personnel, equipment, and facilities of the United States and/or its designated friends and allies. The Department will employ protection capabilities that leverage, complement, and coordinate with capabilities of the U.S. interagency contributors, state, and local government efforts, and friendly nation partners. The Department will lead protection efforts for assigned mission, support protect efforts of other agencies and enable partner nation protection.

Capability Goals (continued)

- **Capability Goals**

  - Protection capabilities development will enhance protection against kinetic attacks (including WMDs), terrorist threats, and threats to nuclear weapons security. Improved coordination capabilities will enable rapid and effective Department participation in consequence at home and abroad

  - The ultimate goal of the holistic approach is to enable Joint Force Commanders to establish and maintain Integrated Engagement Space –volumes of space where appropriate offensive and defense capabilities of the global, regional and local fights are employed to established/achieve desired effects. The layered methods use capabilities to attacks threats either on the ground or in flight, and to mitigate the effects of successful attacks

Goal to ensure commanders at all levels have the necessary equipment, technologies, and capabilities to employ both active and passive defense measures to defeat the threat

Protection SWarF Attributes

- **Effective**
  - **The Joint Force (JF) Must have the ability to bring to bear the capabilities required to prevent/deter, dissuade, defeat or, if necessary, mitigate the effects of an attack. The JF must also have a process and capability for obtaining a desired effect on the enemy that leads to achieving an objective.**
- **Persistent**
  - **JF components must have the ability to operate and survive within their environment, providing an enduring ability to achieve effects. This includes, hardening, use of protective garments to protection from biological and chemical threats, electromagnetic pulse protection, increased system reliability, and logistical support.**
- **Fully integrated**
  - **All protection component capabilities, to include DoD and interagency capabilities must be joint, synchronized, and integrated into a focused efforts with a unified purpose.**
- **Networked**
  - **Systems must be linked and synchronized in time and space to allow dispersed forces to communicate, maneuver, and share a common operating picture.**

Protection Senior Warfighter Forum (SWarF) attributes provide metrics for solutions

Desired Operational Capabilities

Air & Missile Defense (P, M, R&D JCAs)

Area	Future State	Attributes
Air Missile Defense Ballistic Missile Defense	Ensure Joint Integrated Air and Missile Defense against cruise and ballistic missiles	Effective Persistent Fully integrated
Common Operational Picture	Improved common operational picture with automatically fuzzed information from specific sources or data formats in a multilevel security network-centric environment to be able to evaluate, interpret and predict	Persistent Fully integrated Networked
Wide Area Air Surveillance	Improved use of wide-area air surveillance of systems providing surveillance to locate, tag, and track WMD, hostile forces, aircraft, cruise missile and ballistic missiles	Persistent Fully integrated Networked

Desired Operational Capabilities

Air & Missile Defense (P, M, R&D JCAs)

Area	Future State	Attributes
Detection of small, low speed, low-altitude targets	Improved capability to detect small, low-speed, low- altitude targets to adequately protect join maneuver/maneuvering forces from reconnaissance, surveillance, and target acquisition (RSTA)	Persistent Fully integrated Networked
Discrimination for air and ballistic vehicles	Reliably provide adequate tracking information (discrimination) for air and ballistic vehicles	Persistent Fully integrated Networked
Capability to provide time-critical assessments	Improved capability to provide time-critical assessment to permit adequate engagement decisions (use lethal or nonlethal capability or continue to monitor)	Persistent Fully integrated Networked

Desired Operational Capabilities

Combating WMD (M, R&D JCAs)

Area	Future State	Attributes
Combating WMD and homeland defense	Improved nonlethal capability for combating WMD and homeland defense missions	Effective Persistent
Standoff detection of fissile materials	Improved ability to detect fissile materials such as nuclear devices at standoff ranges	Effective Persistent Networked
Standoff detection of CBRNE	Improved standoff detection of chemical, biological, radiological, nuclear, and enhanced high explosive (CBRNE) materials	Effective Persistent Networked
Advanced biotechnology threats	Improved countermeasures against advanced biotechnology threats	Effective Persistent

Desired Operational Capabilities

Combating WMD
(M, R&D JCAs)

Area	Future State	Attributes
Post-detonation nuclear forensics	Develop improve post-detonation nuclear forensics capabilities	Persistent Networked

Desired Operational Capabilities

Protection
(P, M, R&D JCAs)

Area	Future State	Attributes
Counter Improved Explosive Devices (C-IED)	Enhanced protection against IEDs to include detection and neutralization	Effective Persistent
Biometrics and Forensics	Improved identity dominance/biometrics/forensics to locate, tag, track terrorists and WMD in denied areas	Effective Persistent Fully integrated Networked
Force Protection	Improved capability to protect against full array of potential threats, including rockets, artillery and mortar (RAM) projectiles of advanced cruise missiles	Effective Persistent
Critical Infrastructure Protection	Improved capability to provide Critical Infrastructure Protection from terrorists threats and threats from space	Effective Persistent
Ground Vehicle Protection	Improved ground vehicle protection	Effective Persistent

Questions?

BACKUP

Protection Joint Capability Area Attributes

- Effective. The Joint Force (JF) Must have the ability to bring to bear the capabilities required to prevent/deter, dissuade, defeat or, if necessary, mitigate the effects of an attack. The JF must also have a process and capability for obtaining a desired effect on the enemy that leads to achieving an objective. This can be measured by:
  - **Ability to limit collateral damage**
  - **Degree of achievement of a physical, functional, or mission "kill"**
  - **Degree of protection achieved for personnel, physical assets, and information**
  - **Degree of lethal and no-lethal effects inflicted on an adversary for those capabilities required for the protection mission**
  - **Time required from identification of a specific threat to defeat of that threat**
  - **Intelligence gathering: degree of impact and effects of an enemy threat on friendly forces or non-combatants in the operating area**
  - **Quality of and accuracy of information in the knowledge base**
  - **Time required to disseminate and obtain or receive required information throughout the force**

Protection Joint Capability Area Attributes

- Persistent. JF components must have the ability to operate and survive within their environment, providing an enduring ability to achieve effects. This includes, hardening, use of protective garments to protection from biological and chemical threats, electromagnetic pulse protection, increased system reliability, and logistical support. This can be measured by:
  - **Ability of personnel, physical assets and information systems to remain effective in the operational environments**
  - **Percentage of mission capability lost, over time, due to adversary actions**
  - **Time required to restore effective operations after sustaining the effects of an adversary's attack**

Protection Joint Capability Area Attributes

- Fully integrated. All protection component capabilities, to include DoD and interagency capabilities must be joint, synchronized, and integrated into a focused efforts with a unified purpose. This can be measured by:
  - **Degree of protection achieved by the JFC at Point of Embarkation (POE) to the Point of Debarkation (POD) and back (force projection)**
  - **Degree of integration of protection methods incorporated by the JF**
  - **Degree of integration of interagency and multinational participants in protection plans**
  - **Degree of integration of mission technology, and forces to achieve a unified purpose/effort**

Protection Joint Capability Area Attributes

- Networked. Systems must be linked and synchronized in time and space to allow dispersed forces to communicate, maneuver, and share a common operating picture.
  - **Time required from receipt of warning to implementation of protection measures**
  - **Degree of interoperability between actors, including those within DoD and those involving DoD, Law Enforcement Agencies, and international players in protection**
  - **Degree to which an accurate presentation of the battlespace is conveyed to the JF through a common operating picture**
  - **Degree to which information is shared horizontally and vertically**
  - **Time required to identify an enemy threat and provide warning**
  - **Percentage of information exchange requirements met**

Protection in JCA Terms

Tier 2

Tier 3

Prevent (Active Defense)

Prevent Kinetic Delivered Attack

Tier 4/5

- Above surface (IAMD, Counter ASAT)
  - Maneuvering
  - Non-maneuvering
- Surface (Installation Defense)
  - Maneuvering
  - Non-maneuvering
- Sub-surface (Torpedo, MCM)
  - Maneuvering
  - Non-maneuvering

Tier 3

Tier 4

Prevent Non-Kinetic Delivered Attack

- Above surface
- Surface
- Sub-surface

Mitigate (Passive Defense & Consequence Management)

Tier 2

Mitigate Lethal Effects

Tier 3

- Chemical (lethal)
- Biological (lethal)
- Radiological
- Nuclear
- EMP (lethal)
- Explosives
- Projectiles
- Directed Energy (lethal)
- Natural hazards

Tier 4

Mitigate Non-Lethal Effects

Tier 3

- Kinetic munitions
- Chemical (non-lethal)
- Biological (non-lethal)
- EMP (non-lethal)
- Electro-magnetic spectrum
- Direct Energy (non-lethal)

Tier 4

Protection in JCA Terms

Tier 2 Research and Development

Tier 3 Basic Research –

-- The ability to conduct a systematic study directed toward the discovery of knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications

Tier 3 Applied Research

- The ability to conduct a systematic study to understand the means to meet a recognized and specific need

Tier 3 Advanced Technology Development

- The ability to product innovative and unique components and prototypes that can be integrated into defense systems for field experiments and/or tests in a simulated "or operational "environment" to assess military utility" prior to full development.





INTELLIGENCE

SURVEILLANCE

RECONNAISSANCE

ENVIRONMENT

Joint Staff/J28
Battlespace Awareness
Functional Capabilities Board

NDIA 6th Annual Disruptive Technologies Conference

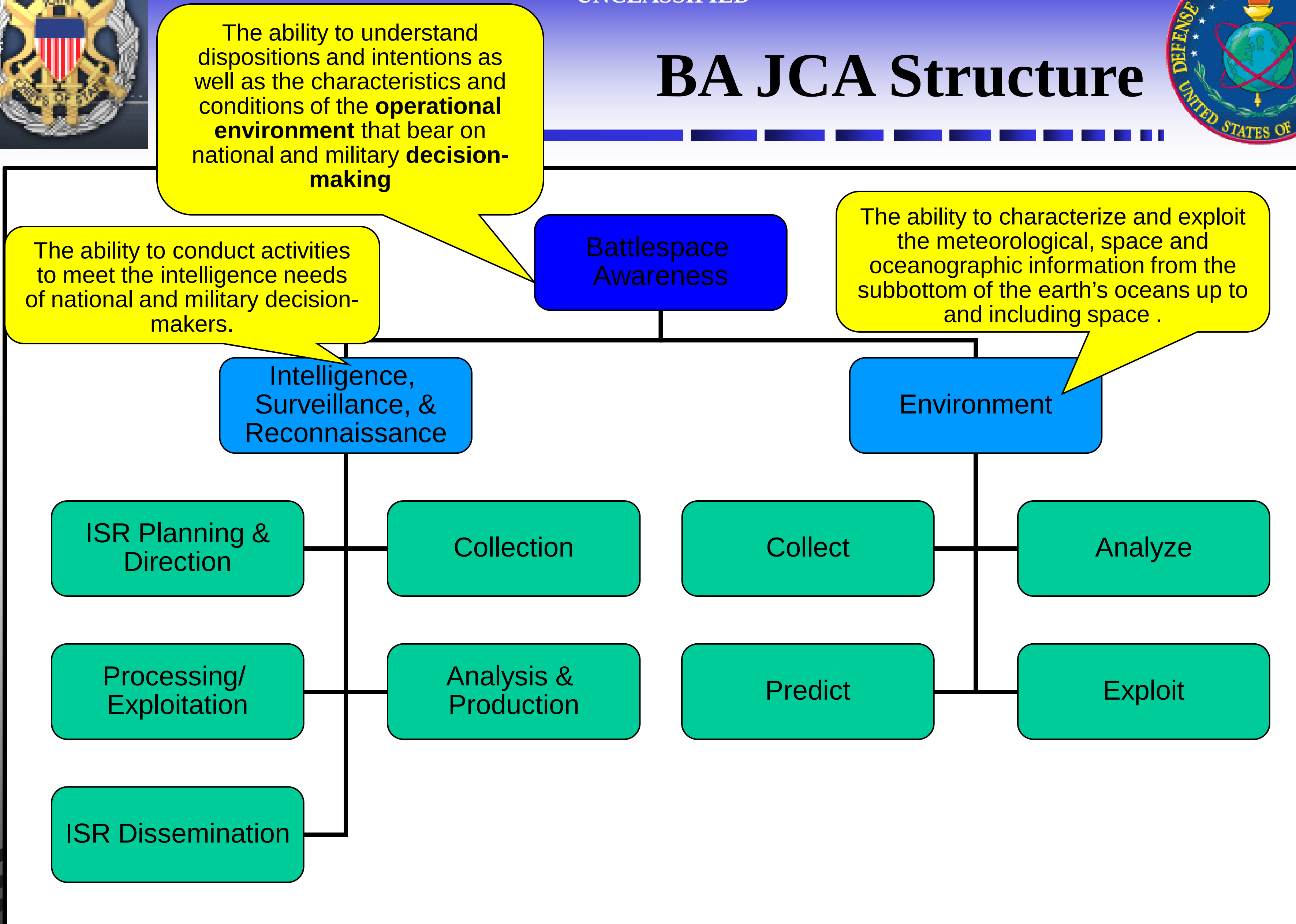
Mr. John Neri
Northrop Grumman/TASC
Programming & Assessments
JS/J282

15 Oct 2009

Overview

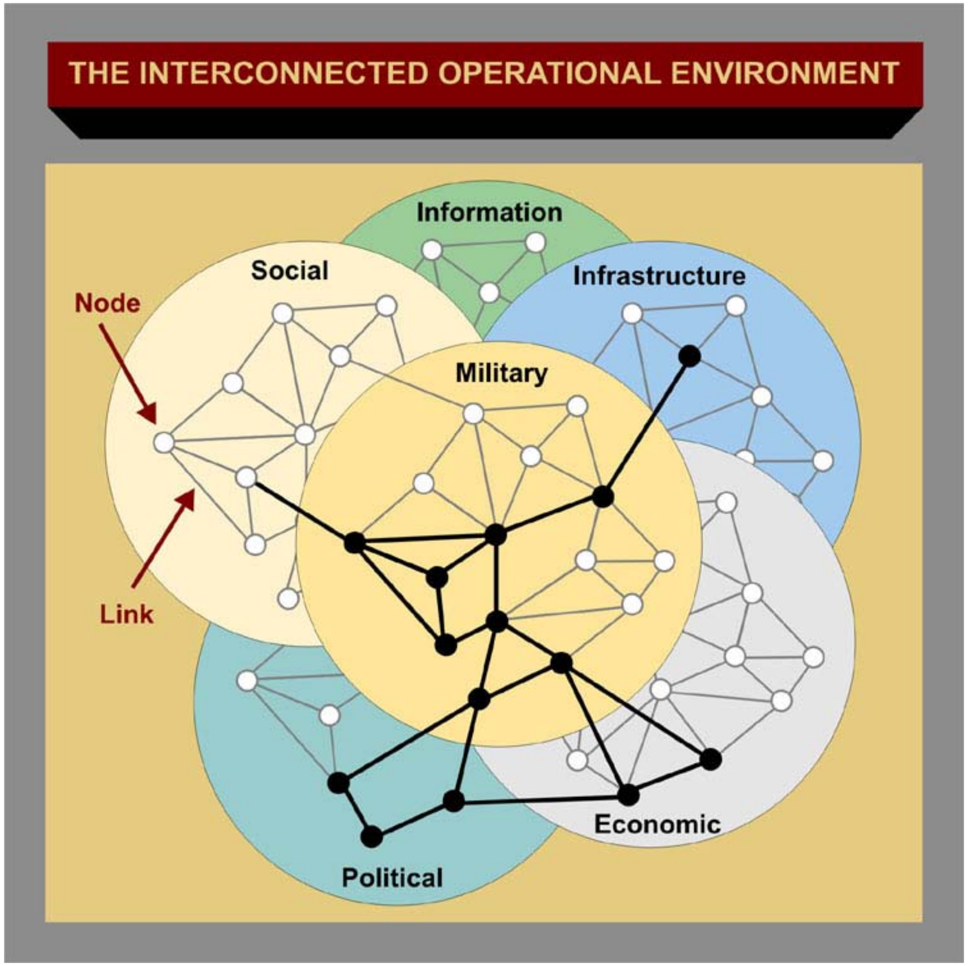
- Battlespace Awareness Joint Capability Area
  - Intelligence, Surveillance, & Reconnaissance (ISR) capabilities
  - Environment capabilities
- Capability Drivers
- Desired Capability Needs
- Questions

BA JCA Structure



The Operational Environment

- Our Battlespace Awareness capabilities must collect and analyze all spheres of the **operational environment**.
- Where can Disruptive Technologies aid in those spheres that the intelligence community has shortfalls?
    - Socio-Cultural
    - Urban Environment
    - Financial
    - Cyber



Process of Interaction

- Intelligence Cycle continues to accelerate as adversary capabilities advance.
- Where can Disruptive Technologies provide our **decision-makers** (White House to the Foxhole) with an advantage?
    - Planning/Tasking
    - Collection
    - Processing
    - Analysis
    - Dissemination

Needed Capability - Long Endurance

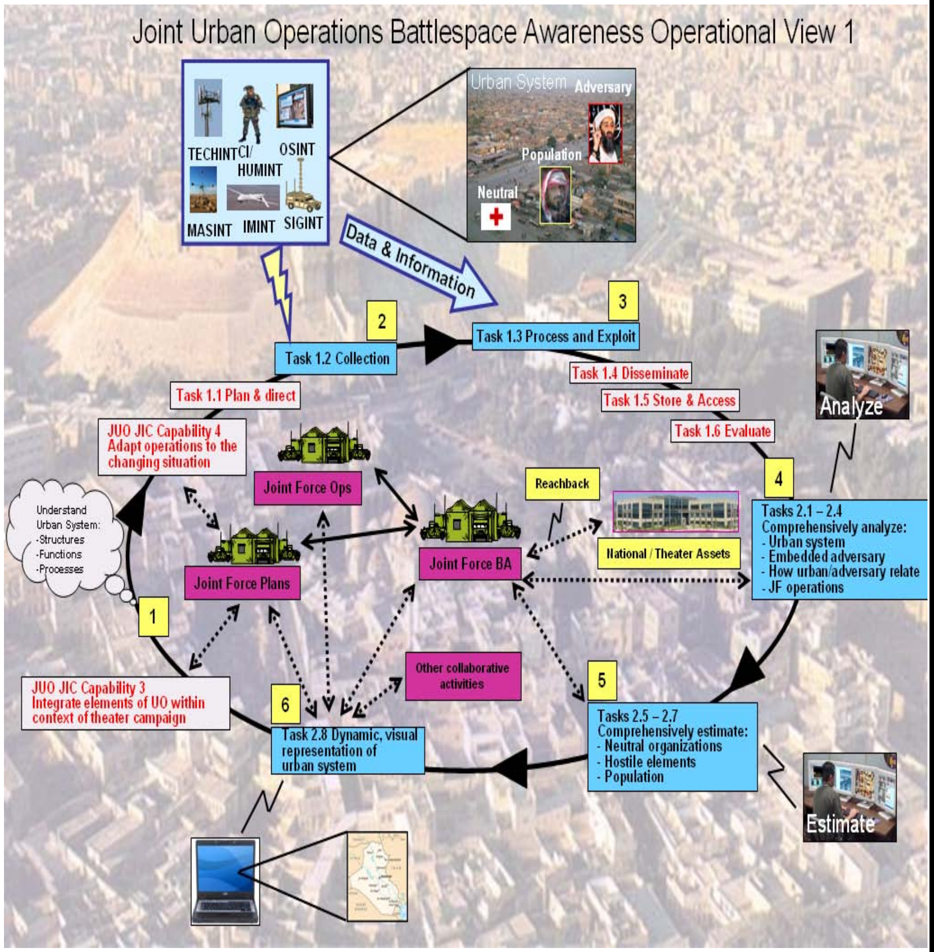
- **Looking for single platform endurance of at least 5 days**
- **Flexible payload: comm relay, EO/IR, SIGINT, WAPS, and SAR/GMTI or combination**
- **Persistent Surveillance with real time/near real time data to the warfighter**
- **Hostile and/or non-hostile airspace**

Needed Capability - Tunnel Detection

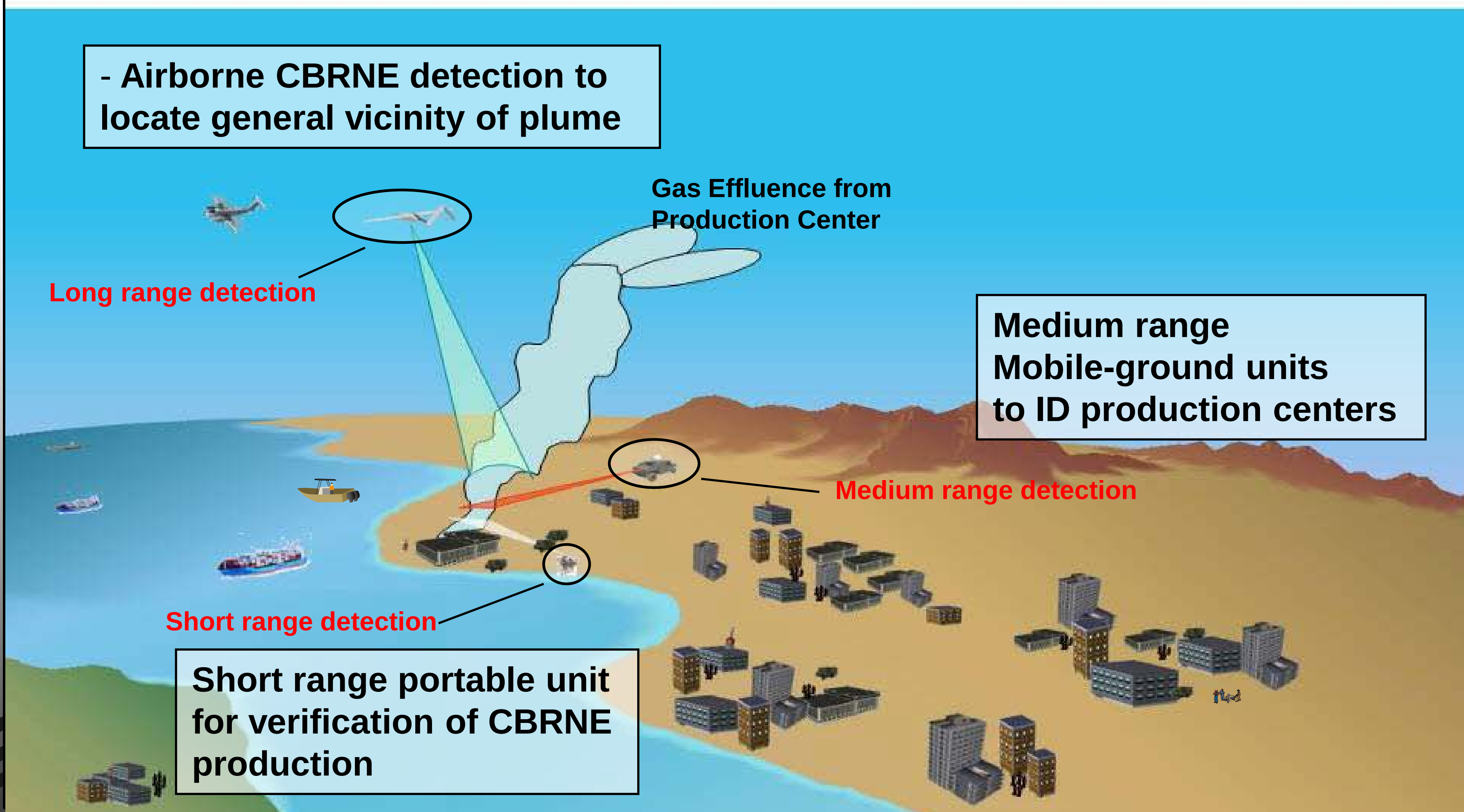
- CONUS
  - 100 cross-border tunnels found since 1990
  - 59 tunnels in Nogales, AZ alone
  - 24 discoveries by Law Enforcement Agencies in CY08
- OCONUS
  - Detainees Tunneling out of OCONUS Theater Internment Facilities (TIFs)
  - Enemy Combatants in AF/PAK region heavily reliant on tunnels

Needed Capability – Socio-Cultural Data (SCD) Collection & Analysis

- Strategic level SCD analysis for Phase 0-1 planning
- Geo-spatially referencing SCD to be available in AOR, down to tactical level
- Work through the security and policy issues surrounding sharing SCD with NGOs, coalition partners, other USG agencies, etc…



Needed Capability – Stand-off Collection/Analysis of CBRNE signatures



Questions?

BACK-UPS

Collection Sub-tiers (1 of 4)

- **Collection** – The ability to obtain required information to satisfy intelligence needs.
  - **Signals Collection** – The ability to gather information based on the interception of electromagnetic impulses, however transmitted.
    - **Communications Signals Collection** – The ability to intercept and derive information from voice and data communications passed by radio, wire, automated info systems/networks, or other electromagnetic means.
    - **Electronic Emissions Signals Collection** – The ability to intercept and derive information from non-communication emitter transmissions.
    - **Foreign Instrumentation Signals Collection** – The ability to intercept data from foreign equipment and control systems.
  - **Computer Network Collection –** The ability to use computer network exploitation (CNE) to gather data from target or adversary automated information systems, networks, and data bases.

Collection Sub-tiers (2 of 4)

- **Collection** – The ability to obtain required information to satisfy intelligence needs.
  - **Imagery Collection** – The ability to obtain information from the visible and non-visible spectrum based on the likeness or visual presentation of any natural or man-made feature, object, or activity.
    - **Electro-Optical Imagery Collection** – The ability to gather information from a visual presentation derived from the ultraviolet through far infrared electromagnetic spectrum.
    - **Panchromatic Collection** – The ability to obtain a visual presentation from the visible spectrum of any natural or man-made feature, object, or activity.
    - **Infrared Collection** – The ability to obtain a likeness or visual presentation from the Infrared spectrum of any natural or man-made feature, object, or activity.
    - **Ultraviolet Collection** – The ability to obtain a likeness or visual presentation from the ultraviolet spectrum of any natural or man-made feature, object, or activity.
    - **Spectral Collection** – The ability to obtain data from reflected or emitted radiation based on the interaction of radiant energy and various materials, using discrete bands across a wide spectral band width.
    - **Light Detection and Ranging Collection** – The ability to obtain information from a visual presentation produced from emitted timed pulses of light.
  - **RADAR Imagery Collection** – The ability to derive information from a visual presentation produced by recording radar waves from a given object within the radiofrequency spectrum

Collection Sub-tiers (3 of 4)

- **Collection** – The ability to obtain required information to satisfy intelligence needs.
  - **Measurements and Signatures Collection** – The ability to collect finite metric parameters and distinctive characteristics of phenomena, equipment, or objects.
    - **Electro-Optical Signatures Collection** – The ability to collect information on phenomena that emit, absorb, or reflect electromagnetic energy in the ultraviolet through infrared spectrum.
    - **Radar Measurements and Signatures Collection** – The ability to actively or passively collect energy reflected from an object to derive information on radar cross-sections, spatial measurements, motion and radar reflectance, and absorption characteristics.
    - **Geophysical Measurements and Signatures Collection** – The ability to detect phenomena and gather information transmitted through the earth (ground, water, and atmosphere) and man-made structures including emitted or reflected sounds, pressure waves, vibrations and magnetic field/ionosphere disturbances.
    - **Radio-Frequency Signatures Collection** – The ability to collect information from radiation transmissions and electromagnetic pulses.
    - **Chemical / Biological Materials Measurements and Signatures Collection** – The ability to gather information to aid in the identification and characterization of chemical and biological objects and activities.
    - **Nuclear Radiation Measurements and Signatures Collection** – The ability to obtain information derived from nuclear radiation and other physical phenomena associated with nuclear weapons, reactors, devices, facilities and fissile materials..

Collection Sub-tiers (4 of 4)

- **Collection** – The ability to obtain required information to satisfy intelligence needs.
  - **Human Intelligence, Surveillance and Reconnaissance Collection** – The ability to acquire information from human resources and human reconnaissance assets.
    - **Interrogation** – The ability to procure information by direct or indirect questioning techniques.
    - **Source Operations** – The ability to develop information through the direct or indirect use and elicitation of sources.
    - **Debriefing** – The ability to obtain information through questioning of cooperating human sources.
    - **Ground Reconnaissance** – The ability to use human resources to obtain, by visual observation and other detection methods, information about activities and resources.
    - **Biometrics Collection** – The ability to gather information on an individual based on measurable anatomical, physiological, and behavioral characteristics.
    - **Media Collection** – The ability to obtain information from acquired, seized or open-sourced hardcopy documents and electronic media

Army
Science & Technology

Michigan Chapter
NDIA
National Defense Industrial Association

National Defense Industrial Association

Technology Opportunities and Challenges

14 October 2009

Dr. Thomas H. Killion
Deputy Assistant Secretary of the Army for Research and Technology/ Chief Scientist

Predicting the Future

It's tough to make predictions, especially about the future. Some famous technology predictions include:

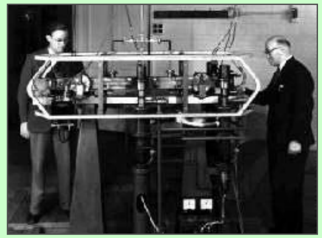
- ***"Heavier-than-air flying machines are impossible."***
  - ***Lord Kelvin, 1895***
- ***"Airplanes are ...of no military value."***
  - ***Marshal Ferdinand Foch, 1911***
- ***"Who ... wants to hear actors talk ?"***
  - ***H. M. Warner, 1927***
- ***"... (T)here is world market for maybe five computers."***
  - ***T. Watson, IBM Chairman, 1943***
- ***"640k (RAM) ought to be enough for anybody."***
  - ***Bill Gates, 1981***

Disruptive Technologies

Decade of the 1950's

Lasers

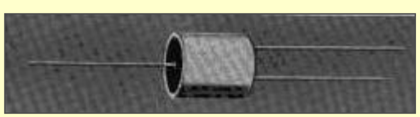
Atomic Clock



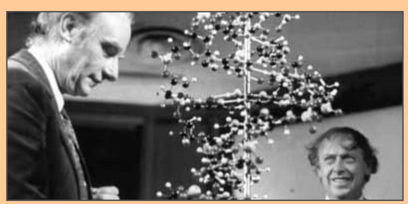
Programmable Systems

WWII Ballistic Computing/ ENIAC

Transistor

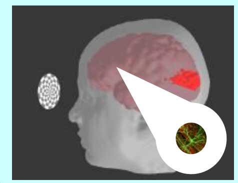


DNA



Today for 2020 and beyond…

Functional Brain Imaging & Beyond

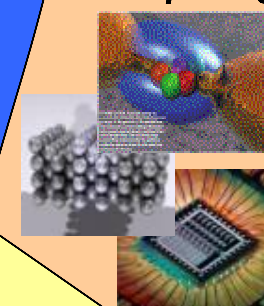


Robotics

Nano-technology

Network Science

Quantum Computing



Immersive Environments

Bio-technology

Future Army Soldier—1956

Laminated steel and plastic helmet

Radio transceiver inside helmet

Plastic armor choker

Plastic armor tunic (zippered on the sides and bottom with overlapping shielding at fastened points)

Ammunition pouches

Wearing a scientifically designed helmet, plastic armor tunic and ultra-light equipment, this Futurarmy soldier will move and fight with greater ease and efficiency than any other soldier in modern history. The helmet visor will not only offer added protection but will provide the soldier with night vision and telescopic sight. Manning a variety of missiles and other weapons, this Futurarmy soldier of the 1970s will be the best protected individual since knights wore steel armor.

38 ARMY ■ November 2006

"Army Magazine" Vol 56. No.11 p.38, November

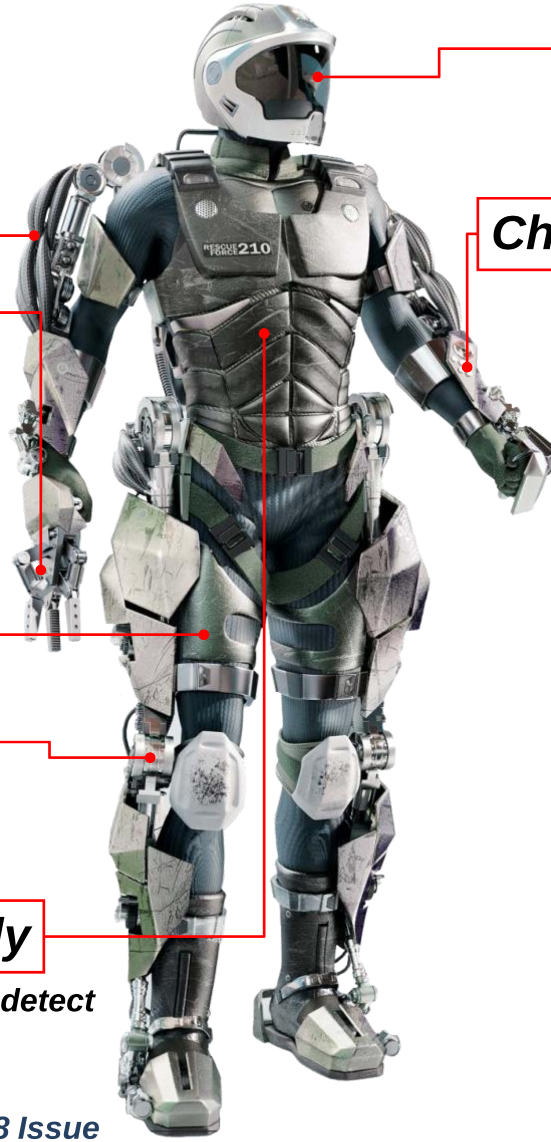
Throat microphone and chin strap

Pocket for cigarettes or personal items

Emergency Rations

Ammunition

Soldier—2020



Lift Five Tons

Develop new polymers that produce force 100 times that of a natural muscle

Wield Any Weapon

Variety of manipulators that enable handling of complex weapons

Walk Into Bullets

Although an exoskeleton could support heavier armor, a lower weight solution is in the works

Run Like an Olympian

Motion similar to the way we walk

Heal Wounds Automatically

Sensor and smart suit that would detect and treat injuries

Monitor Systems Status

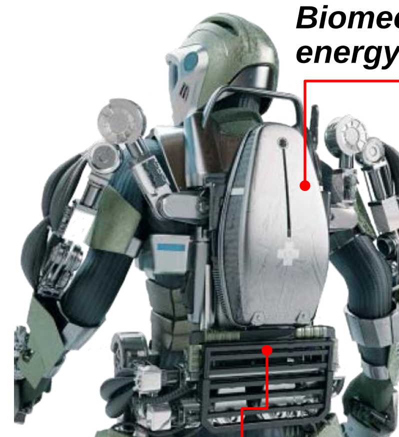
Helmet mounted display

Change Functions Immediately

Suit that tailors efficiency for type of activity -- short sprints or long distance walks

Power Itself

Biomechanical energy creation



Evacuate Anyone

Fold down platform that injured soldiers could sit on so that they can be carried out

Popular Science May 2008 Issue

Major Trends Affecting Future Systems

- *Computers will almost disappear and be embedded in everything*
- *Further advances will be made in light-emitting devices that are highly efficient and printable*
- *Very complex robotic systems will be developed to think, learn, and perform human and non-human tasks faster and better*
- *Nanotechnology, Biotechnology, and Miniaturization will lead to major advances in medicine, manufacturing and the environment*
- *Virtual environments will be indistinguishable from reality*
- *We will understand how the human brain works*

Army S&T…
Engine of Transformation

Telcordia. the elements of success

Developing Secure & Resilient Next Generation Communications Networks & Services

Prepared for:

Disruptive Technologies Conference

Telcordia Contact:
John Kimmins
Executive Director/Fellow
jkimmins@telcordia.com
732-699-6188

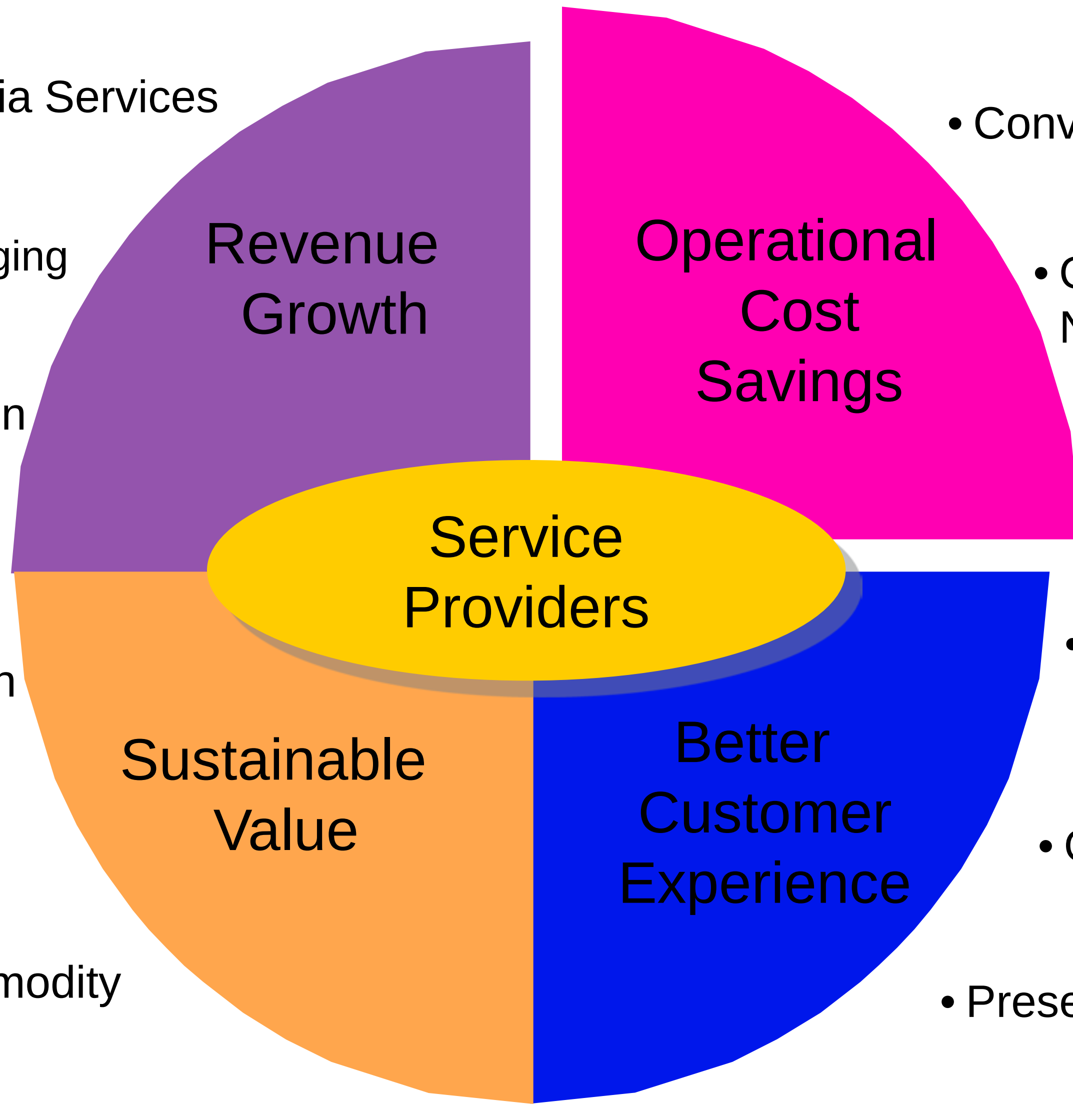
Overview

- Network & Services Transformations
- Security Threats
- Technical & Operations Trends
- Current Security Approaches
- Risk Management Framework

Network Transformation:
Market Drivers

- New Multi-Media Services
- Service Based Charging
- Rapid Service Creation

- Converged Call Control
- Open, Standards-based Network
- Less Operations Staff

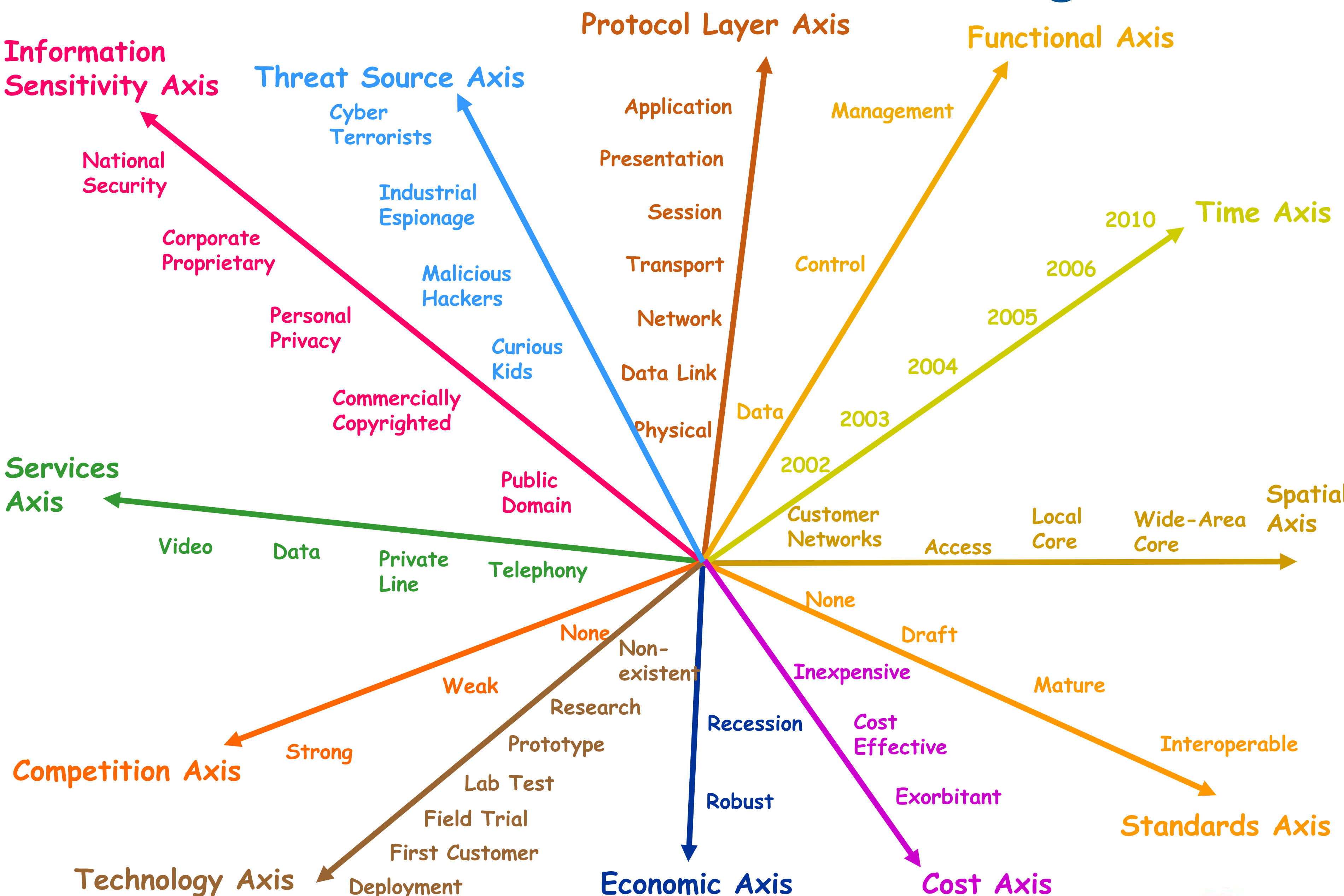


- Sell Services, not an "IP pipe"
- Services = Value
- Transport = Commodity

- Access Agnostic (e.g., mobile, fixed, wireless)
- Greater User Control
- Presence & Availability

Telcordia.

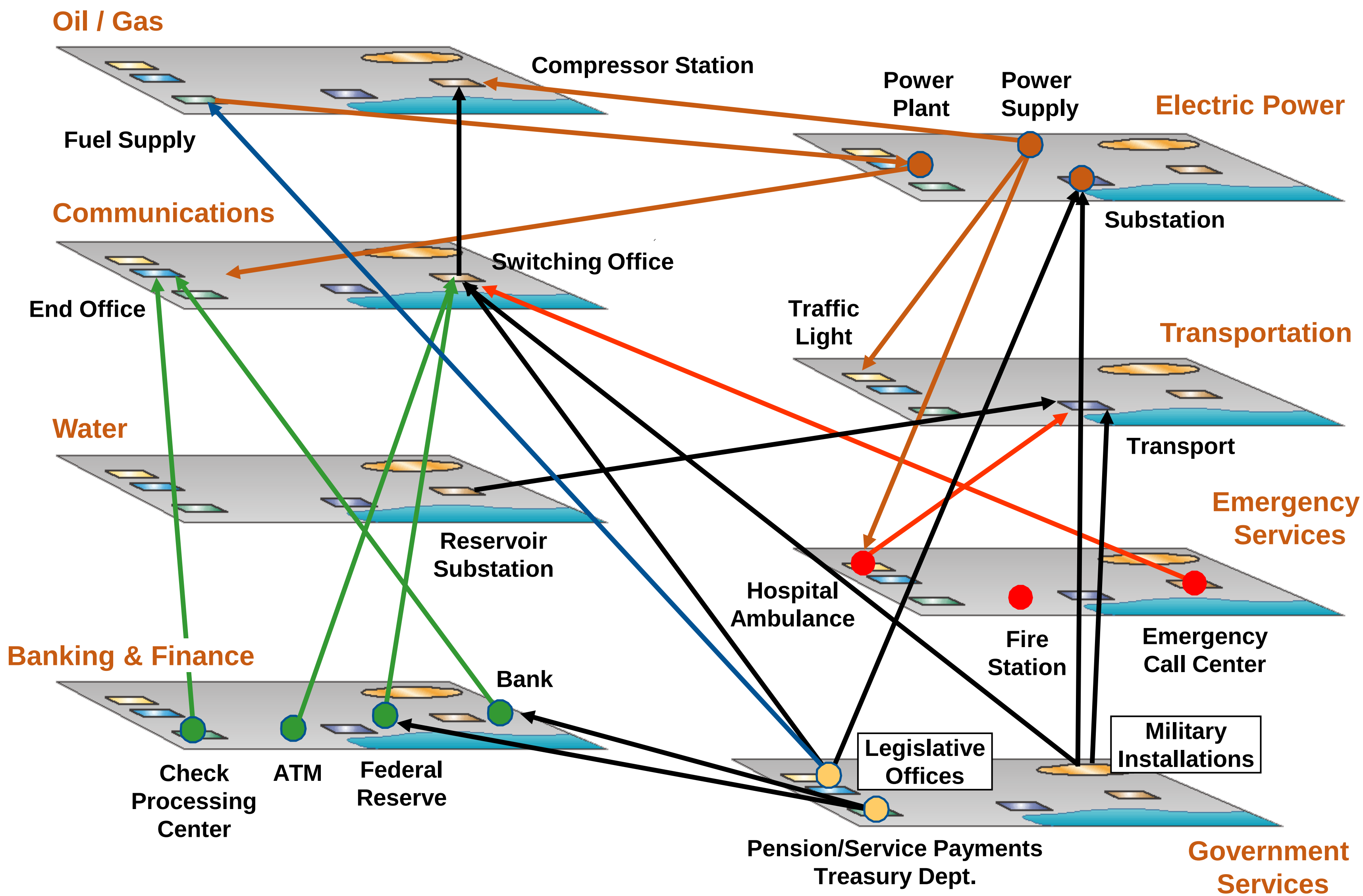
Multi-Dimensional Challenge



Telcordia.

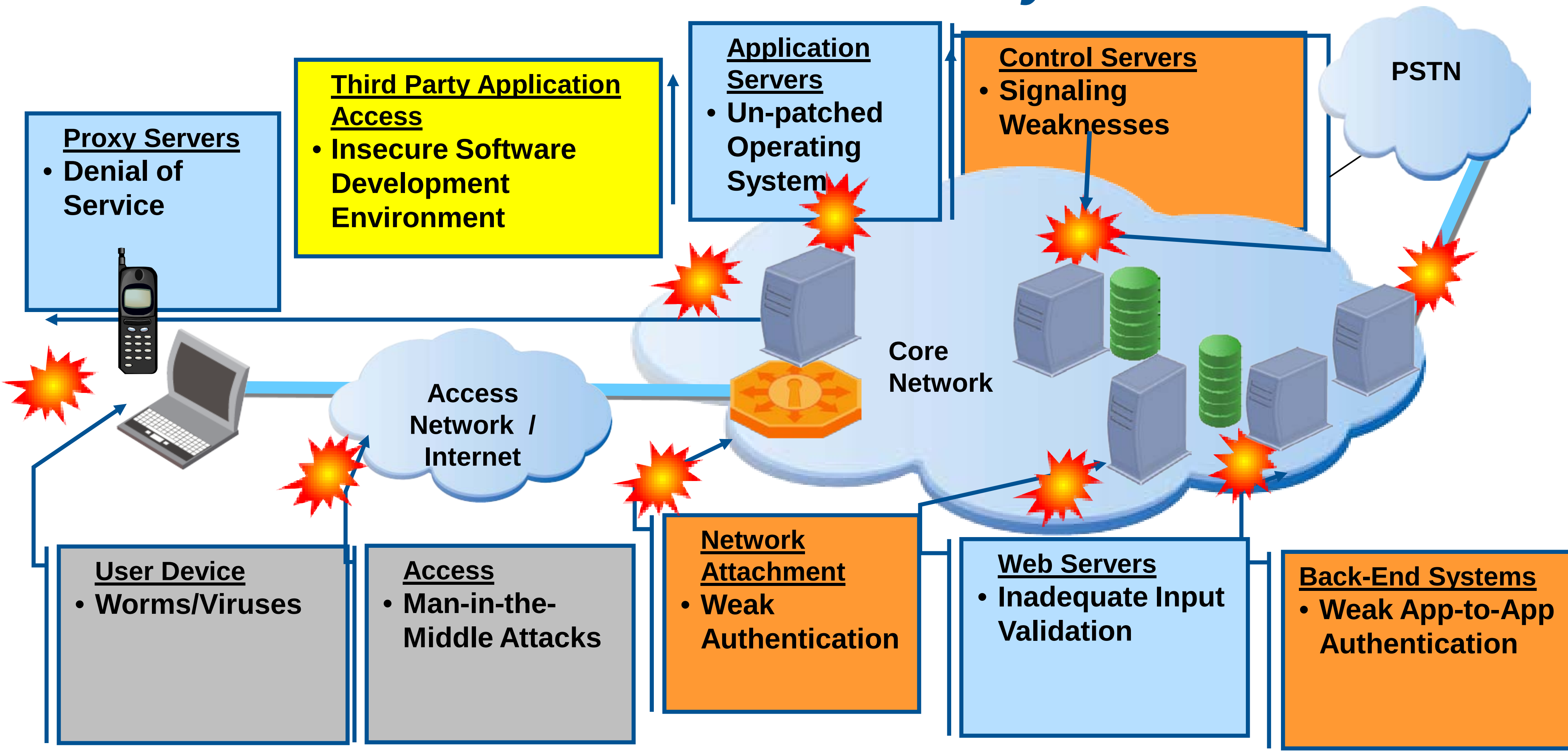
Threats Magnified

Interdependencies & Technology Evolution



Telcordia.

Network Transformation:
End-to-End Infrastructure Security Risks



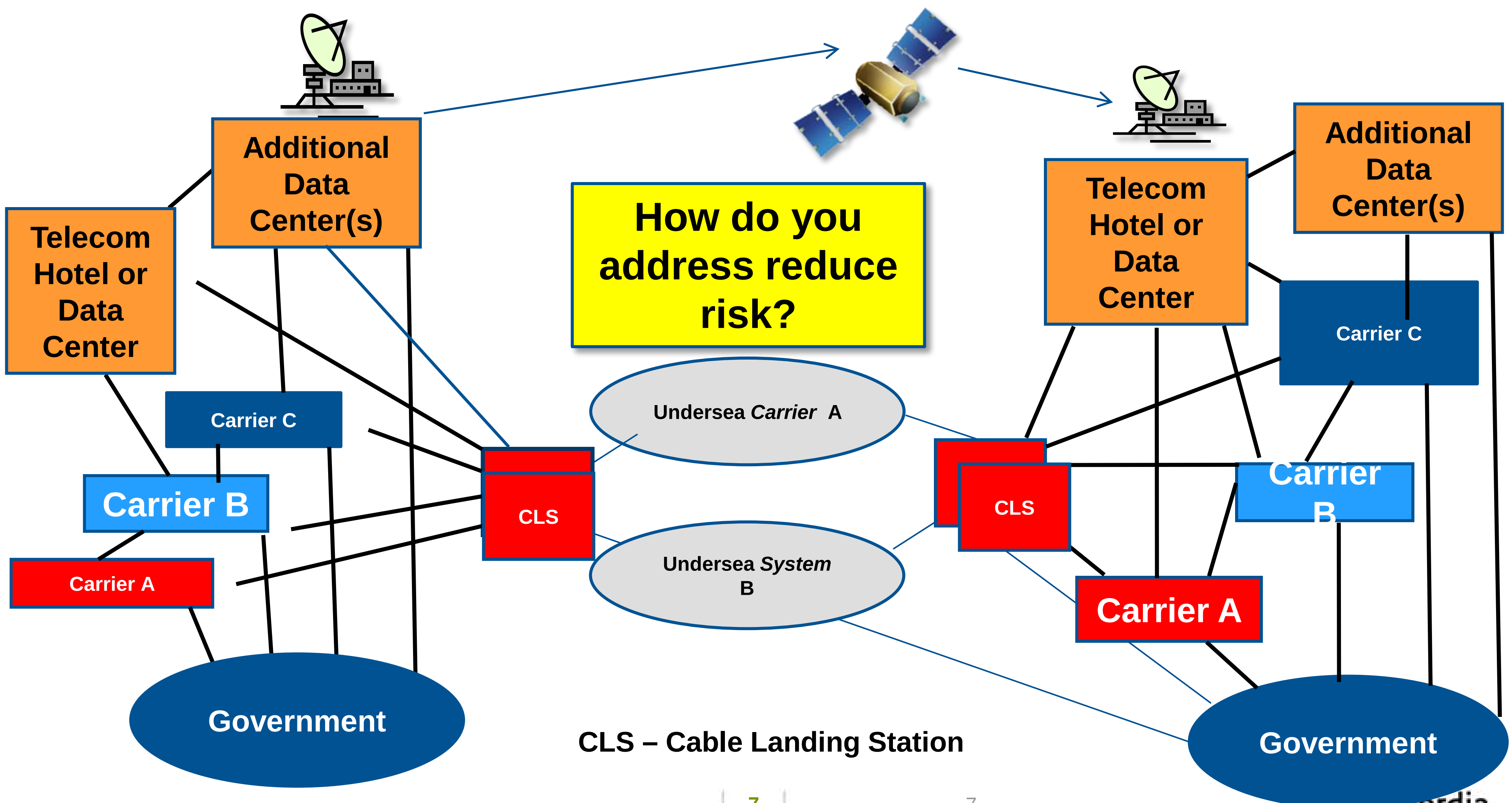
Security Legend

(light blue)	IT Servers	(orange)	Core Network
(yellow)	Applications	(grey)	Access

Telcordia.

Network Security & Resiliency Under Attack

"Take Balad Air Base, for example," Colonel Fielden said. "A passing ship anchor cut an undersea fiber optic cable and Balad went from conducting hundreds of combat sorties per day to conducting tens of sorties a day. What do you do when communications systems are down? Not much of anything."



CLS – Cable Landing Station

Next Generation Network (NGN) Deployments

How is Security today?

- **Basic**
  - Baseline security requirements for product vendors are vague
  - Organizational issues are not fully identified and addressed
- **Not mature**
  - Security performance and reliability are critical elements and need to be improved
  - Signaling and media security are not fully recognized by the market
  - Integration of security functionality still evolving
- **Poorly planned and implemented**
  - Implementations inherit traditional vulnerabilities (e.g. Buffer Overflows)
  - Security features to enforce stronger security posture (protocol, user and boundaries) are not uniformly implemented

Need to address both NGN and Legacy Network Security

Evolving Wireless Networks & Services

- Besides handset applications there are *new* applications and services infrastructures emerging
  - Vehicle Telematics
    - On-board computers with multiple wireless interfaces
    - Roadside wireless networks
    - Vehicle to Infrastructure & Vehicle-to-Vehicle communications
  - Smart Grid Energy Management Systems
    - Networks linking entities and devices (e.g., sensors, meters) for generation, distribution and usage
    - Automated smart meter management

Wireless Telematics

In-Vehicle System

- In-Vehicle Telematics Architecture
- Applications Software
- Security & Privacy Management

Multi-Mode Access

- GPRS
- EVDO
- HSDPA
- DSRC

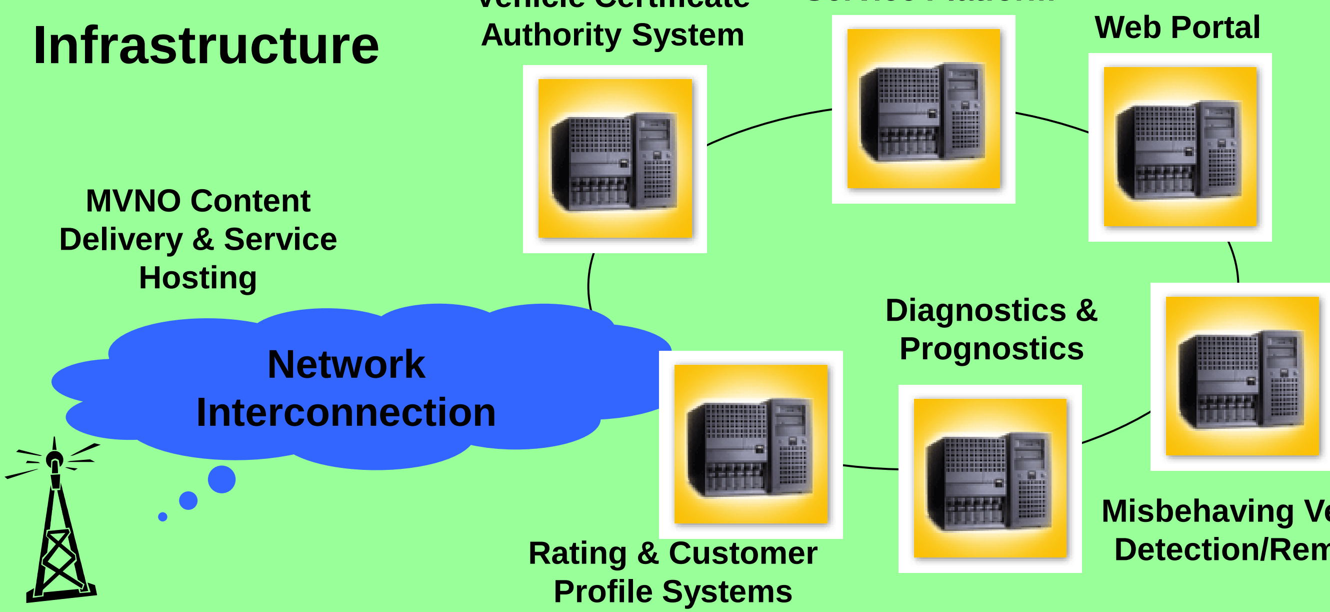
- WiFi
- WiMAX

- Seamless Mobility
- Secure Mobile IP Sessions
- Integrating Emergency Services / Crash Notification Routing

Potential Products & Services

- Telematics Portal
- Vehicle Communications & Network Security
- Telematics Application & Software Development
- Vehicle Diagnostics & Prognostics
- Service Provisioning & Support Systems
- MVNO Content Delivery & Application Hosting
- Transportation Research, Analysis & Modeling

Telematics Network Infrastructure

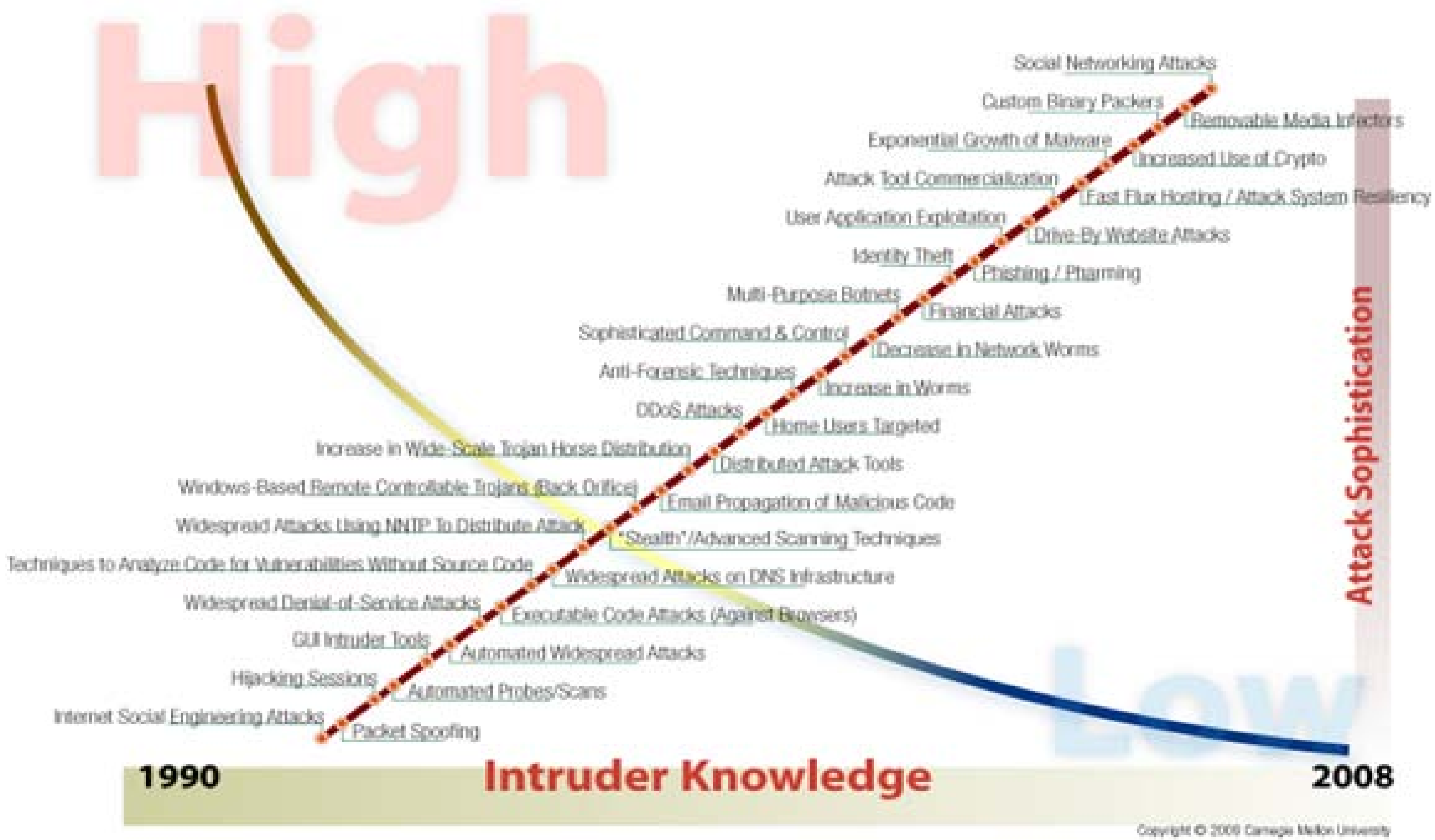


Smart Grid – What is It

- Transform existing energy services using communications technology
  - Remote connects/disconnects
  - Distribution automation
  - Customized user services & billing
- Components
  - Business applications – e.g., generation/supply, SCADA, Usage/demand
  - Computing/IT – e.g., Servers, Web technology, Smart agents
  - Communications Infrastructure – e.g., Home Access Network, WIMAX, Cellular
  - Energy Infrastructure – e.g., Smart Meters, Transformers

Threat Trending

New Targets: Smart phones, STBs, WiFi, Meters, OBEs, etc.



Telcordia.

Technical Trends

- Web-based applications & services
- Mobility with different roaming patterns
- New types of intelligent devices
- Signaling extended out to user
- Multi-media protocols
- Third-party software & user interfaces
- Hardware and software security components

What is Sufficient Security?

Security Testing Evolution

Pen Testing is not sufficient

- **Trend towards embedding security functionality into software and hardware with an increasing threat in software/hardware hacking tools**

Protocol Layers

VoIP Application Layer
(Call Managers, SDPs, PSXs…)

VoIP Protocol Layer

Signaling Protocols
(SIP, H323, SS7…)

Transport Protocols
(RTP, UDP, …)

VoIP Supporting Services Layer
(DNS, NAT, QoS, AAA…)

OS and Network Layer
(Linux, Unix, Windows, ARP, MAC, IP…)

Hardware Layer
(Server, SIP hardware)

Verify proper operation through a wide array of vulnerability analysis tools and techniques

Intelligent User Devices

Embedded Hardware Security Perspective

- Reverse engineering circuit board hardware and firmware
- Exploiting on-chip debugging, JTAG, and in-circuit emulator capabilities
- Accessing and reprogramming FLASH, RAM, and other storage devices
- Stepping, tracing and altering program execution
- Monitoring and inserting data on system and peripheral interfaces
- Extracting / altering keying material, unit identity and other credentials
- Testing PKI functions, such as firmware signatures
- Modifying the circuit hardware to add new devices, remove existing devices, and create new external interfaces
- Re-configuring hardware to masquerade as a different system element

Set Top Boxes

OBE for Vehicles

Smart Meters

3G, ISM Wireless

Operational Trends

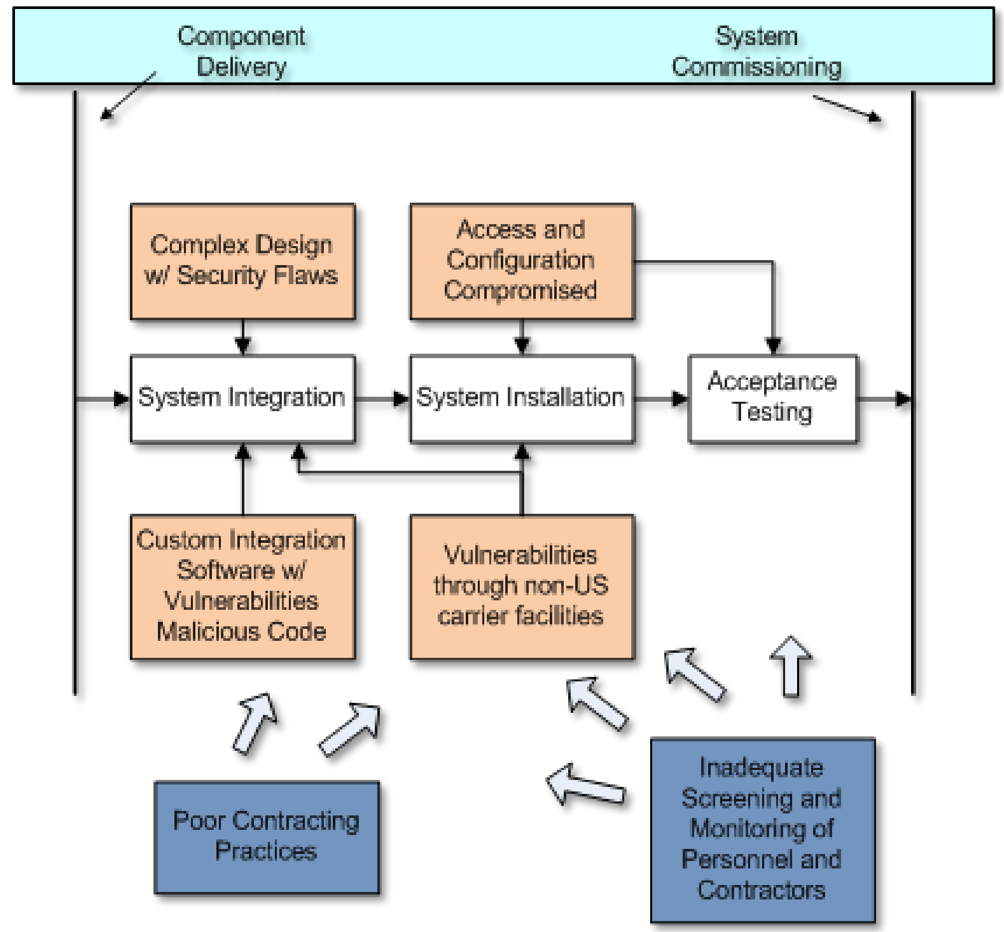
- Primary & Backup NOCs
  - Foreign based NOCs
- Outsourced staff
  - NOC staff
  - Software development
- Lifecycle security across multiple suppliers
  - Supply chain risk management
- Supplier maintaining equipment
- Physical co-location

What is
Sufficient Security?

Supplier Assurance

Need for Visible Risk Mitigation Activities

- **Address the insertion of foreign made COTS into networks by feasible architectures, operations, testing & procurement processes**



Telcordia.

Current Approaches to Address Challenges

They all have Problems

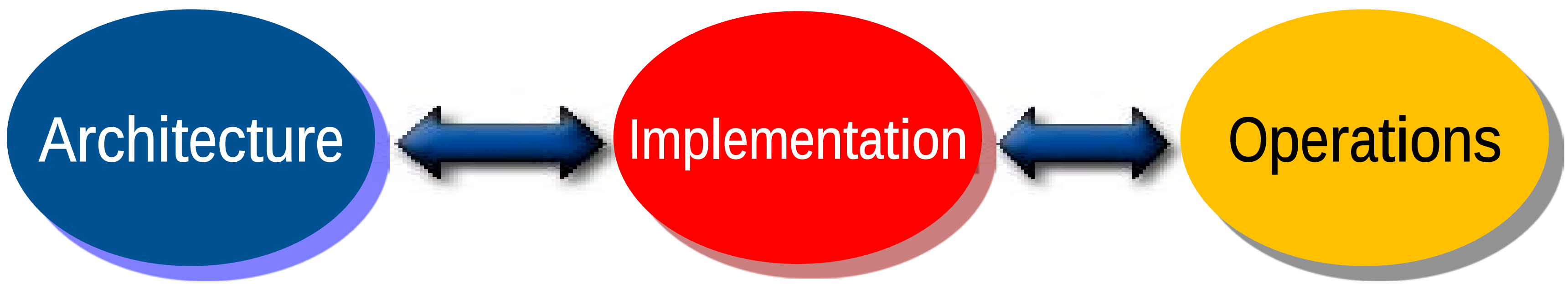
- Secure Remote Access
- Token-based Access
- Personnel Vetting
- Network Partitioning
- Software & Hardware Testing & Analysis
- Trusted Source Software Releases
- Network Traffic Monitoring
- Filtering Inbound and Outbound Traffic
- Site Inspections
- Physical security assessments

Risk Management Framework
Structured Analysis

- **Network/Service Access Security**
  - User and Device Authentication
  - Personnel & Physical Access Profiles
- **User Platform Security**
  - Hardware/Software Security
  - Management and Services Interfaces
- **Application Security**
  - Service logic integrity and interfaces
  - Information Protection End-to-End
- **Core Network Security**
  - Intra and Inter-Network Security
  - Communications among systems & entities
  - Operational security roles and policy considerations

Holistic Life Cycle-based Security Approach

Broader than IT and Truly End-to-End



- User & Network Authentication
- Integrity & Confidentiality of Signaling and Media
- AAA Architecture
- Management Infrastructure
- Traffic Separation
- Protocol Weaknesses (e.g. SIP)
- Network Resilience
- Maturity/Immaturity of Standards

- Service-Level Security
- Platform Weaknesses & Equipment Shortcomings
- Web Application Vulnerabilities
- Security Policy Enforcement
- 3rd Party Application Interface Vulnerabilities
- Information sharing
- Service Disruption/DoS
- Non-Traditional Vendors
- Software Integrity

- Monitoring for Security, Service Assurance, QoS
- Component Configuration Management
- Vulnerability & Patch Management
- Intrusion Detection & Response
- Maintenance Access
- Physical Security
- Authentication Key Management

Disruptive Technologies Conference
14 October 2009
Dr. Larry Schuette

DIRECTOR OF INNOVATION

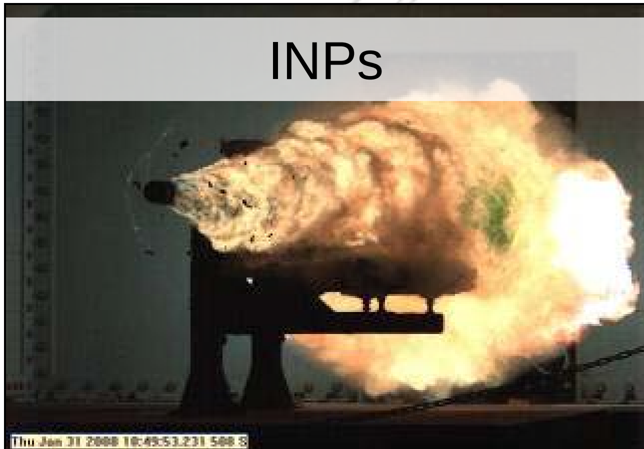
ONR

Dist Statement A: Approved for public release; distribution is unlimited.

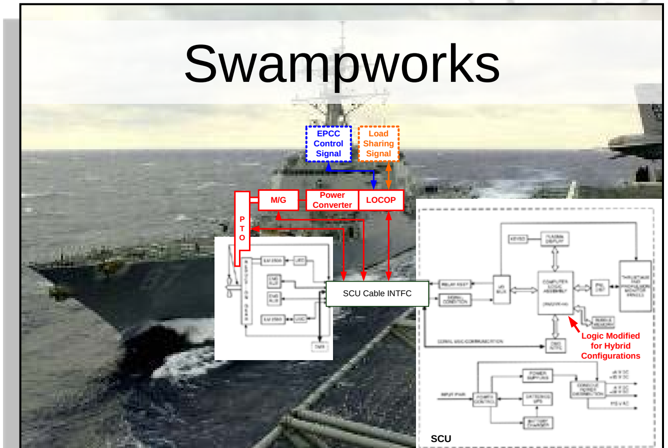
Director of Innovation Portfolio

DIRECTOR OF INNOVATION

Next Big Thing



Disruptive



Sustaining

Disruptive

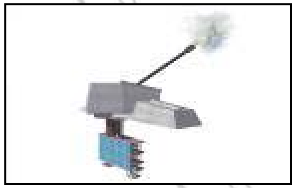
INP Programs Snapshot

DIRECTOR OF INNOVATION

- **Guidance**
  - Innovative and game-changing
  - High risk, high payoff
  - Useable prototype available at completion
  - Deputy PMs from acquisition PEOs to facilitate transition

$1,162M
Planned / Proposed
FY09-15

Current INPs



EMRG

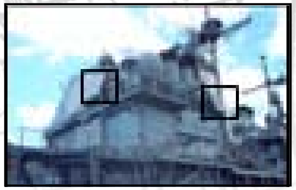
SBE

TACSAT

PLUS

FY-10 INPs

FEL



INTOP

INP Program Status (Current, FY10 New Start, and FY12 Proposed INPs)

DIRECTOR OF INNOVATION

- **Naval Aviation Enterprise**
  - Durable Aircraft
  - Large Format Infrared Focal Plane Systems
  - Naval Variable Cycle Engine Technology
- **Surface Warfare Enterprise**
  - Free Electron Laser (FY-16)
  - Damage Control Technologies for the 21st Century (DC-21)
  - Electric Warships
  - Maintenance Free Ships
- **Undersea Warfare Enterprise**
  - Persistent Littoral Undersea Surveillance (FY-12)
  - Large Displacement Unmanned Undersea Vehicles
  - Supercavitating Weapon
- **Naval Netwar/FORCEnet Enterprise**
  - Integrated Topside (FY-16)
  - Tactical Satellite (FY-10)
  - Integrated Distributed Electronic Warfare Capability for Electromagnetic Spectrum Control
  - SATCOM Vulnerability Mitigation Using Multi-beam Phased Arrays
  - UV Sentry
- **Naval Expeditionary Combat Enterprise**
  - EM Railgun INP Phase I (FY-11)
  - Sea Based Enablers (FY-12)
  - EM Railgun INP Phase II
  - Autonomous Aerial Cargo/Utility System (AACUS)
  - Hybrid Heavy Lift Airship
  - Ultra Heavy-lift Amphibious Connector

*Programs in Red are existing programs – (End Date)

SwampWorks Program Purpose

DIRECTOR OF INNOVATION

ONR

- To develop and demonstrate newly invented or recently discovered technologies that address emergent and enduring operational problems in an accelerated timeframe.

- To develop prototypes of recent technology breakthroughs for experimentation to satisfy war-fighter requirements.

- Pilot disruptive and open innovation processes and tools with the objective of decreasing the time and cost of producing innovative solutions

SwampWorks/Experimentation Program Status (FY09)

DIRECTOR OF INNOVATION ONR

- **Surface Warfare Enterprise**
  - High Temperature Superconducting Degaussing
  - Future Naval Maritime Laser Weapon System Electric Warships
  - Full Ship Shock Trials (FSST) Alternatives
  - Flight Deck Thermal Management System (JSF)
  - SHIPBOARD ENERGY STORAGE (DDG 51 class)
  - HYBRID DRIVE DYNAMIC CONTOLS (DDG 51 class)
  - Advanced Watertight Door Seal
  - Emergent Critical Laser
- **Undersea Enterprise**
  - Advanced Communications at Speed and Depth
  - Large Displacement Unmanned Undersea Vehicles Hybrid Tail Cone
  - Structural Acoustics Detection & Classification For Shallow Water ASW
  - Blue Dart UUV Detection
  - Submarine Payload Door Electric Actuator
- **Naval Aviation Enterprise**
  - Fuel Cell Powered Long Endurance UAS
  - Black Dart (UAS project)
- **Naval Netwar/FORCEnet Enterprise**
  - Maritime Domain Awareness
  - Tactical Satellite (FY-10)
  - Transportable Electronic Warfare Module
  - Long Range EO/IR/LRF Sensor System
- **Naval Expeditionary Combat Enterprise**
  - Operational Adaptation
  - Counter Terrorism Integration
  - High temperature flight deck non-skid experiment (V-22)
  - Hyper Spectral Imagery Of Littoral Terrain
  - Stop Rotor UAS

*Programs in Red are proposed programs for FY10

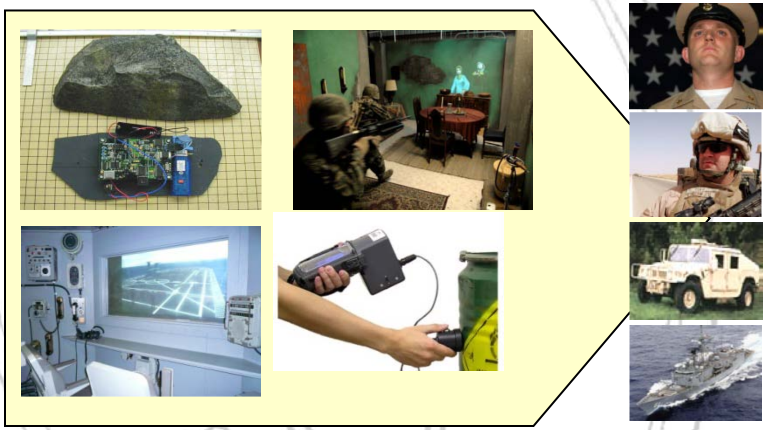
TechSolutions Overview

DIRECTOR OF INNOVATION

Objective
Provide rapid-response S&T solutions to immediate deck-plate level issues in response to Warfighter requests.

Goal
Develop applications of existing and emerging technologies to meet high-interest, near-term Fleet/Force needs; demonstrate prototype solution within 14 months of request.

Warfighters



Platforms

Technical Approach
- Solicit operational needs from Fleet/Force members
- Define solution requirements
- Develop solutions through NRE partners with Fleet/Force feedback early and often
- Transition solutions to PORs, F/F, etc.

S&T Products
- Prototype demonstrations
- Test and evaluation results

Primary S&T Focus Areas
- Naval Warfighter Performance & Protection
- Affordability, Maintainability & Reliability
- Assure Access & Hold at Risk

Example Products
- Infantry Immersive Trainer (IIT)
- Improved WAF Interface Card
- Gun Use Monitoring System for Howitzers
- Sub-Launched UAV (Transition to Flight)
- Portable Acoustic Contraband Detector

FY09 TechSolutions Projects by Enterprise

DIRECTOR OF INNOVATION

- **Naval Aviation Enterprise**
  - HCO Tower Simulator
  - Non-pyrotechnic SAR marker
  - Catapult CSV Calculator
  - Tool Room Management System
  - MRT3 Training Keyset
- **Surface Warfare Enterprise**
  - EW Target Mapping Toolkit
  - AIS Identity Validation Tool
  - Defense Against Terrorist Tactics
- **Undersea Warfare Enterprise**
  - Solid State Lighting for Subs
  - Non-traditional Hull-mount Sensor
  - CASS Software Update
  - WAF Output to SMMTT and A-TAS
  - Submarine Exercise Treadmills
- **Naval Netwar/FORCEnet Enterprise**
  - *none*
- **Naval Expeditionary Combat Enterprise**
  - Mobile Modular C2 in MRAP
  - Imaging Through Walls
  - Powered Rope Ascender
  - Talon Robot Battery Replacement
  - Naval Expeditionary Virtual Training Environment (NEVTE)
  - Infantry Immersive Trainer (IIT)
  - M777 Brake & Shock Sensors
  - Condition-Based Maintenance for Howitzers
  - SDV Waterproof Transport Canister
  - SDV 360-degree Sensors
  - Enhanced Lightweight UUV *(pending)*
  - M203 Indirect Fires Sight *(pending)*
- **Provider Enterprise (NAVSUP)**
  - Food Service Management Software Replacement *(pending)*

DIRECTOR OF INNOVATION

QUESTIONS???

Larry Schuette

Office of Naval Research

larry.schuette@navy.mil

National Defense Industrial Association

Disruptive Technologies Conference

14 October 2009

The Honorable Zachary J. Lemnios

Director, Defense Research and Engineering

Our Guidance

- **Defense Budget Recommendation Statement**
  Secretary of Defense Robert M. Gates, April 06, 2009
  - ***reaffirm our commitment to take care of the all-volunteer force***
  - ***rebalance this Department's programs***
  - ***institutionalize and enhance our capabilities to fight the wars we are in today and the scenarios we are most likely to face in the years ahead***
  - ***provide a hedge against other risks and contingencies***
  - ***fundamental overhaul of our approach to procurement, acquisition, and contracting***
- **Economic Club of Chicago**
  Secretary of Defense Robert M. Gates, July 16, 2009
  - ***What is needed is a portfolio of military capabilities with maximum versatility across the widest possible spectrum of conflict***

DDR&E Imperatives

1. **Accelerate delivery of technical capabilities to win the current fight.**
2. **Prepare for an uncertain future.**
3. **Reduce the cost, acquisition time and risk of our major defense acquisition programs.**
4. **Develop world class science, technology, engineering, and mathematics capabilities for the DoD and the Nation.**

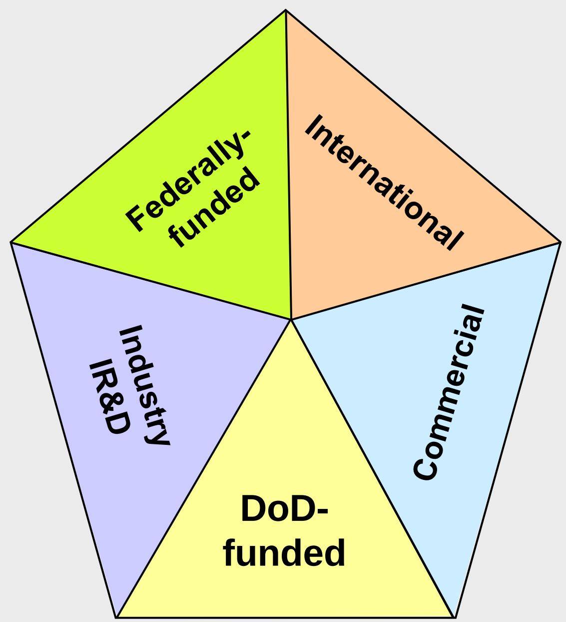
The Challenge Space

UNDERSTAND THE LANDSCAPE

Changing World

Dynamic Threat Space

Evolving Technology



INVEST WHERE WE MUST

LEVERAGE EVERYTHING ELSE

DoD Capabilities

DoD Industrial Base

DoD Core Technologies

Comments from COCOMs

"We need to detect IED's at range… I am willing to test technologies in the field… We need persistent communications on the move…"

"I need the 70% solution today, rather than the 100% solution in 5-8 years…"

"…we are concerned about our technological edge against a near peer competitor…"

"It took us 10 years to get to the Moon, we are 8 years into our research efforts for defeating IED's…we need to find a solution to reliably detect and defeat IED's at range…

"I like the 1 year acquisition cycle rather than the standard 5-8 year cycle, get the prototypes into the hands of the warfighters, turn the feedback into a quick redesign and deliver relevant capability now…"

"Often times we fail due to shortage of imagination…"

The Big Three

Innovation

Speed

Agility

Perspective for the Next Decade

1950 1960 1970 1980 1990 2000 2010 2020

National Security Challenges

Cold War

Vietnam War

Desert Storm

Collapse of Soviet Union

Bosnia

Kosovo

OIF

OEF

Irregular/Hybrid Warfare

Defense Capabilities

ICBM

Satellite comms

C4ISR

Precision Strike

UAV

LGB's

GPS

Stealth

Robotics

Nuclear propulsion

Night Vision

Human Terrain

Ubiquitous Observation

Contextual Exploitation

Scaleable Action

Enabling Technologies

Transistor

Composite Materials

MEMS

Solid state laser

Superconductors

Space tracking

Web protocols

VHSIC

MIMIC

Digital computing

IR Sensors

High Performance Computing

- Advanced Electronics, Photonics Algorithms, MEMS
- Nano; Meta; & New Materials
- Cognitive Computing
- Bio-Revolution

Forces of Change…
Irregular and Hybrid Warfare

Operations in Austere Locations

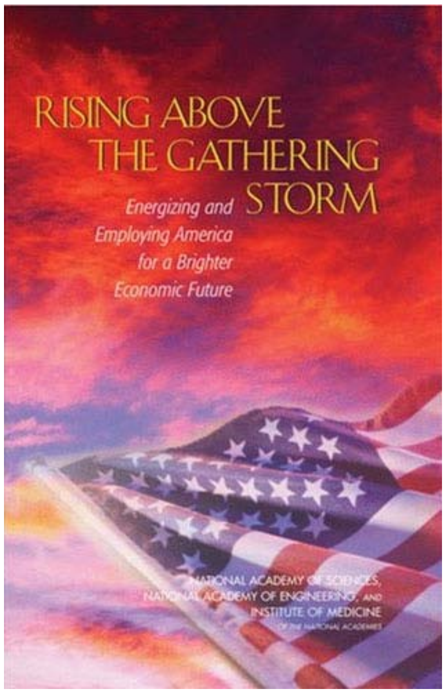
Defense S&T for Persistent / Irregular Warfare

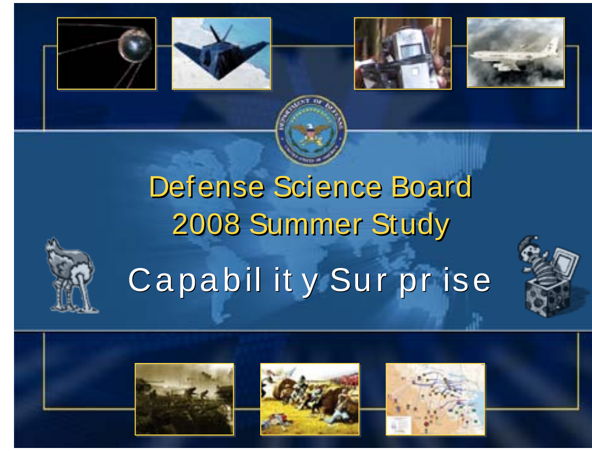
Humanitarian Assistance / Provincial Reconstruction Teams

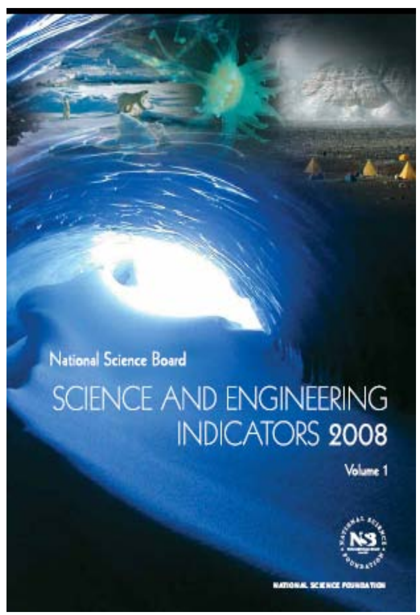
NEW TECHNOLOGY NEEDED

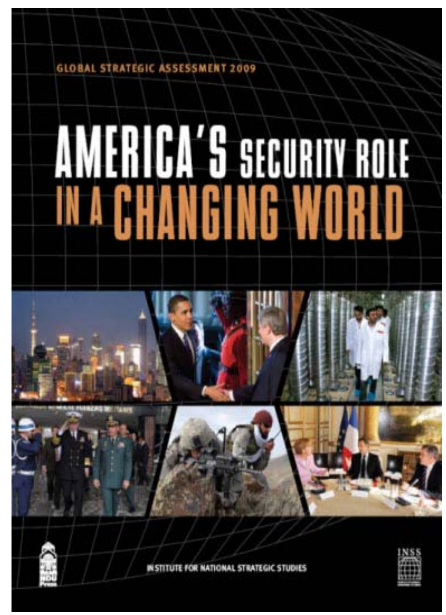
Affecting the Hearts and Minds…

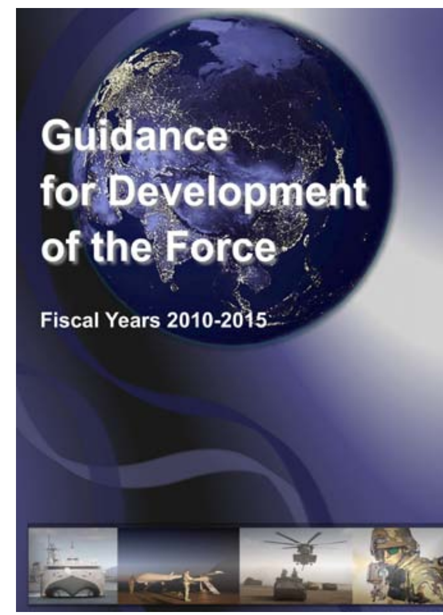
Some Common Threads



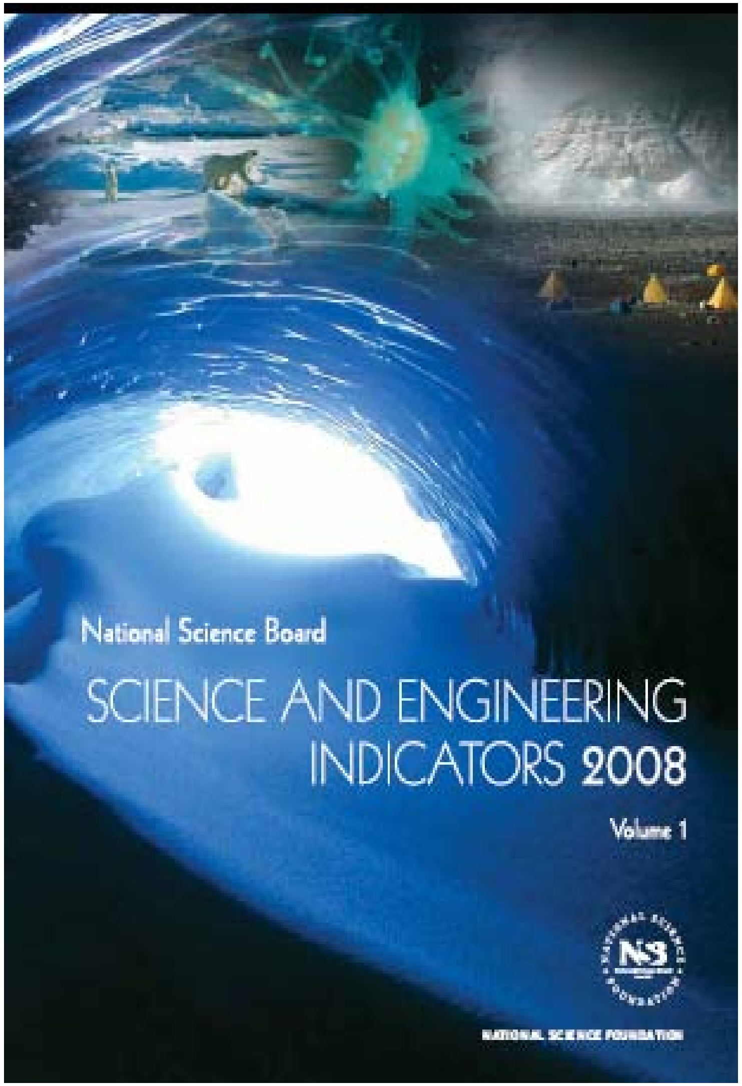






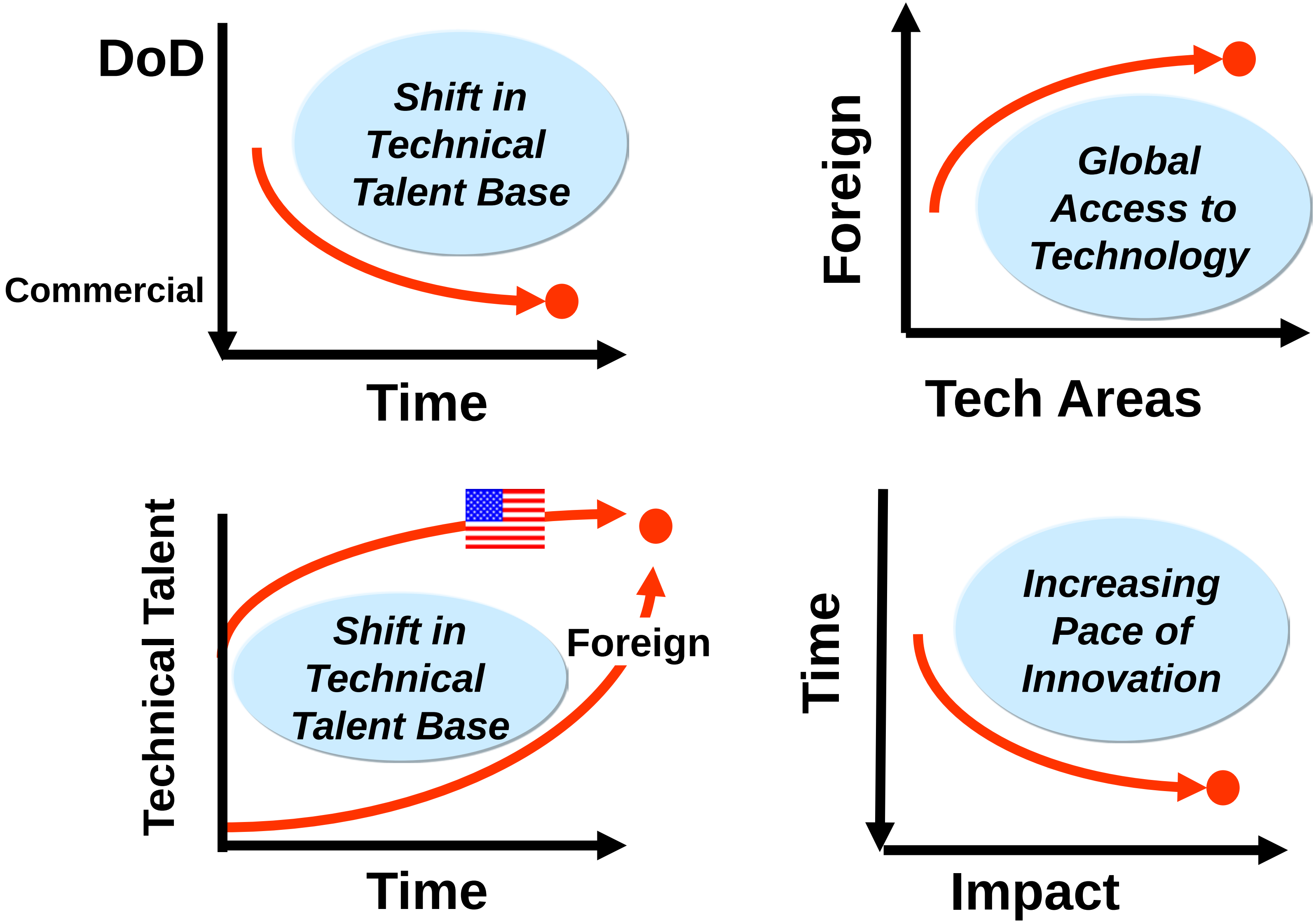


Concerning Trends



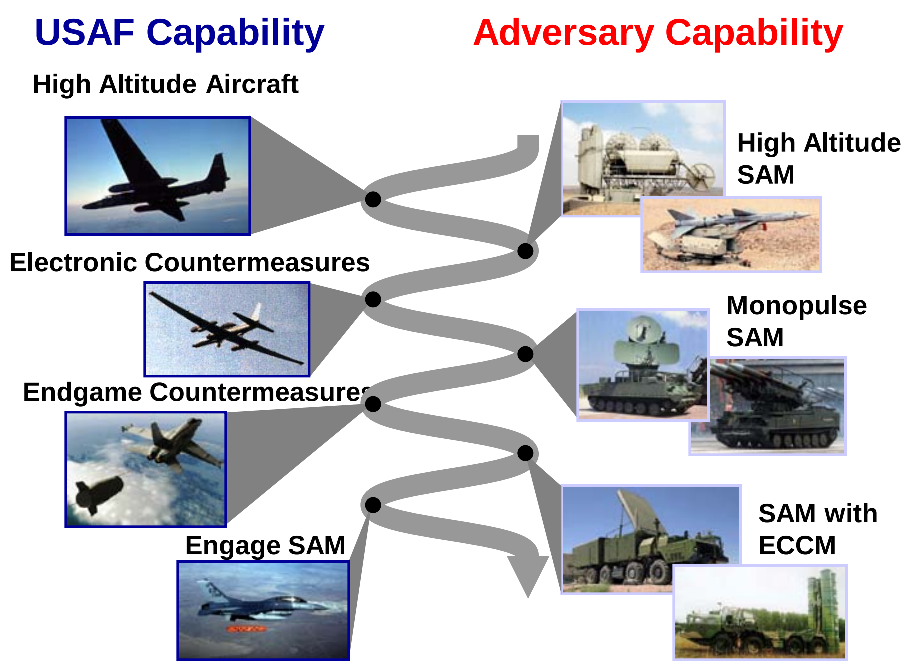
- Knowledge-intensive industries are reshaping the world economy.
- Industry R&D in manufacturing and services is expanding and increasingly crossing borders.
- R&D in the United States is robust and dominated by industry.
- Advanced training in natural sciences and engineering is becoming widespread, eroding the U.S. advantage.

Four Key Challenges to our Technical Base



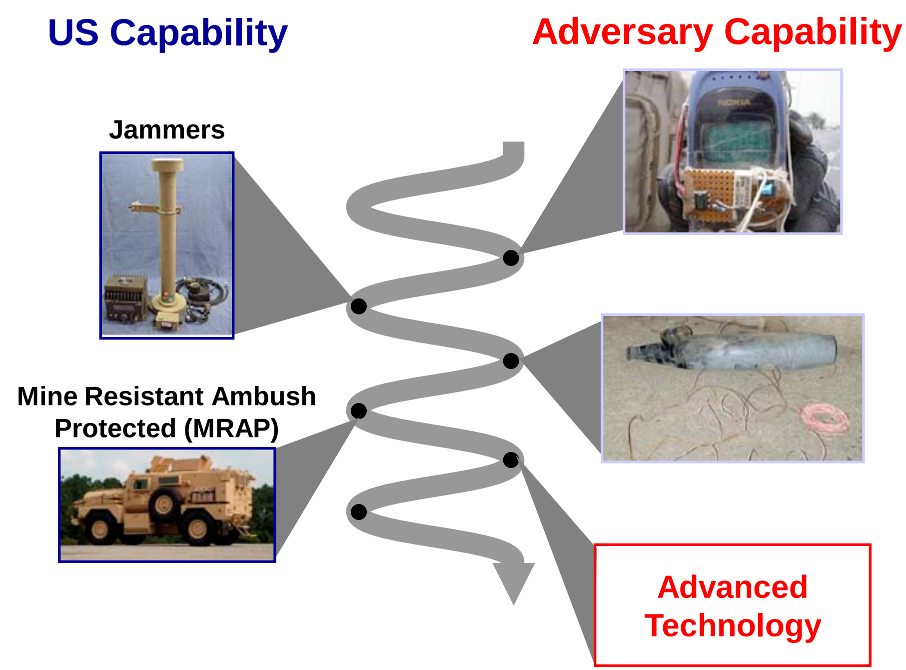
The Timeline has Collapsed!

Conventional Warfare



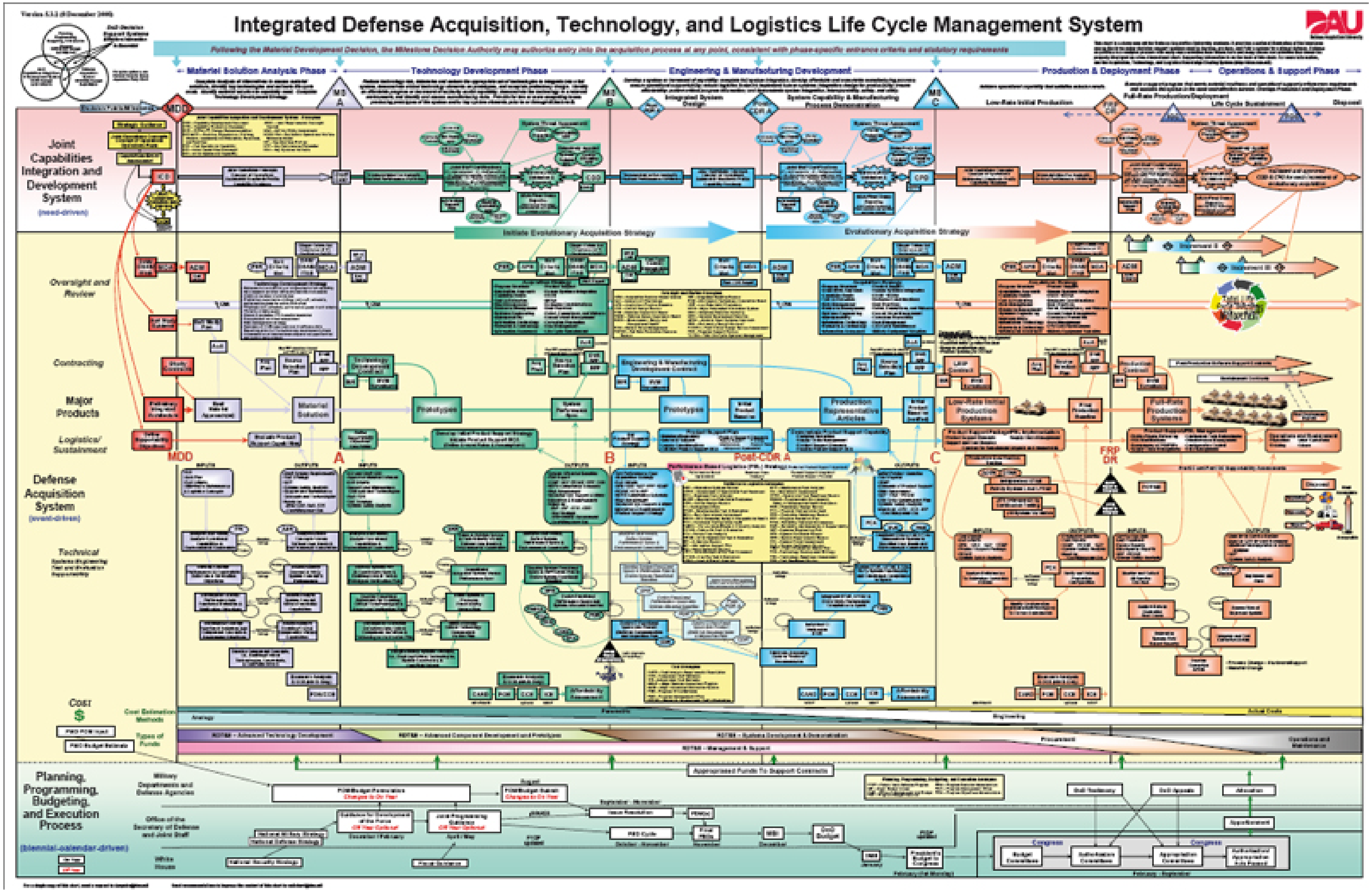
Response loop measured in years

Counter-Insurgency Warfare

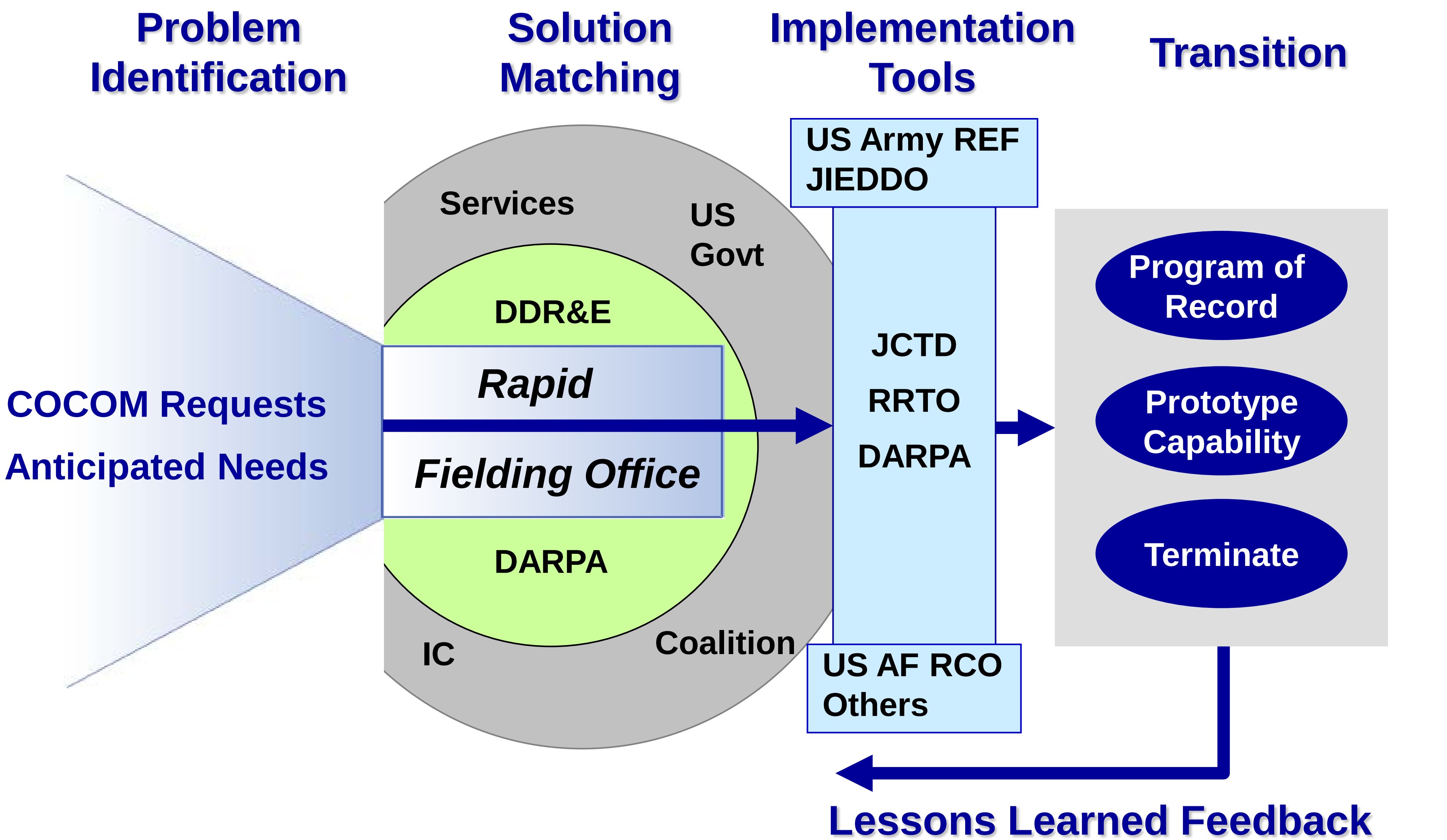


Response loop measured in months or weeks

An Effective Process for Major Defense Systems – but not for Disruptive Technologies



Accelerate Delivery of Capabilities: 6-12 months from concept to capability

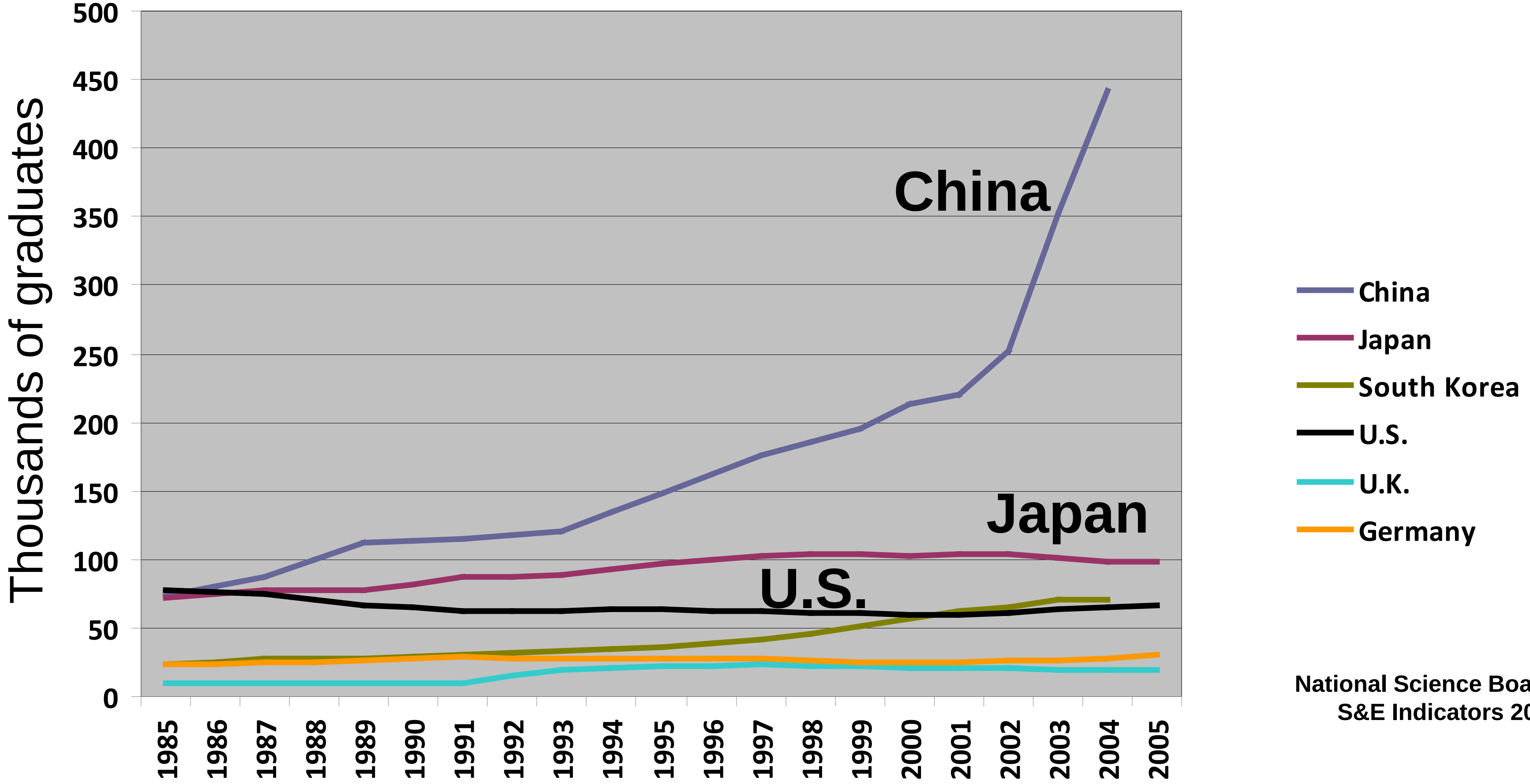


Major Shifts In The Department Of Defense

- **Significant shifts in operational needs**
  - More complex operations (coalition, logistics challenge)
  - Shift in operations from Iraq to Afghanistan
  - Preparedness for disaster relief
  - Energy and environmentally-aware focus
- **Emerging threats**
  - New class of maritime threats (piracy, DF-21, SSN26)
  - Global asymmetric threats
  - Global cyber threats
  - Proliferated WMD
  - Adversary's exploitation of commercial technologies
- **Acquisition**
  - Getting it right
  - Competition for budget
  - Rapid capability to the warfighter

Engineering Graduate Global Competition: Numbers Matter

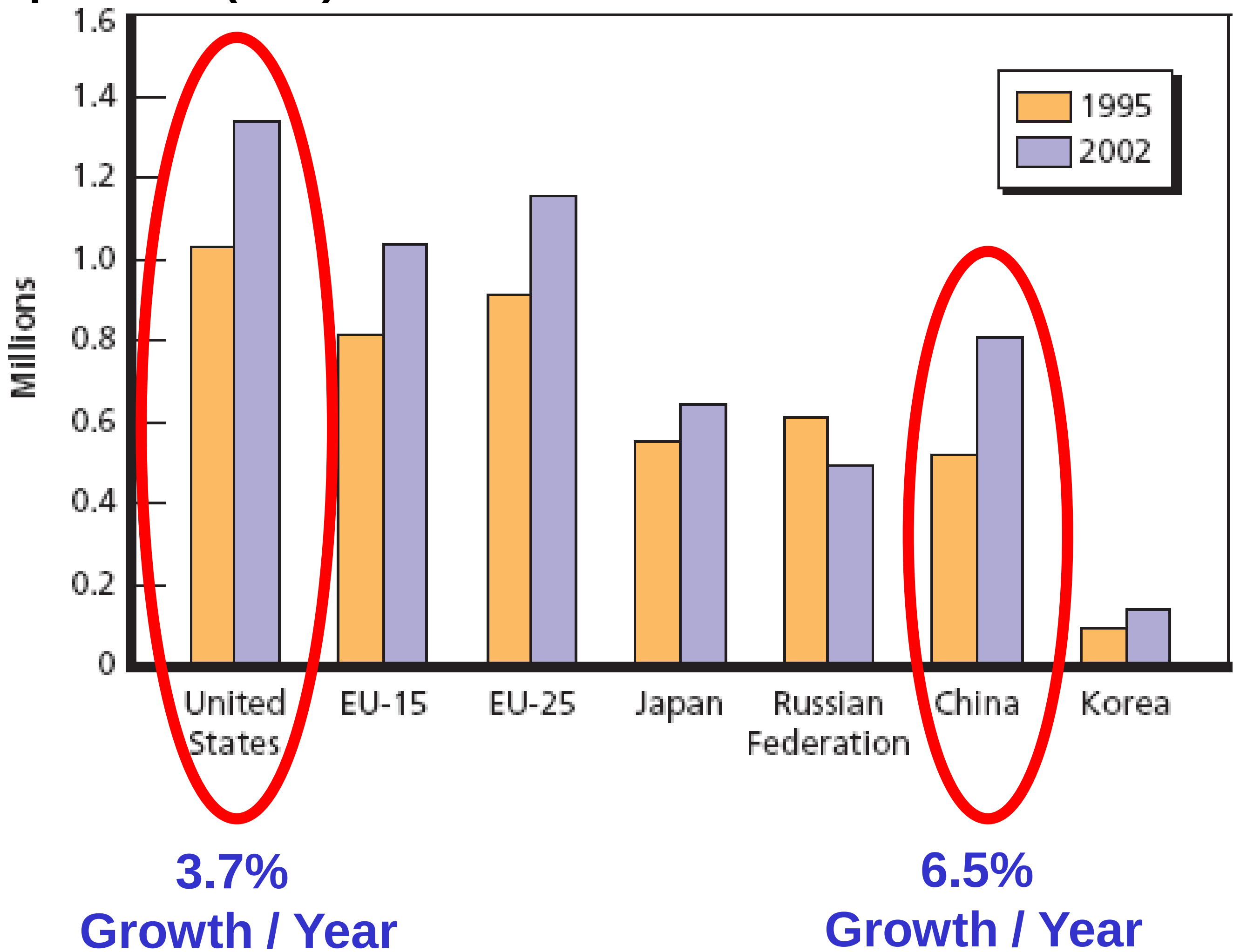
First engineering degrees by country (1985 – 2005):



National Science Board, S&E Indicators 2008

Private Sector Research Workforce: The Shifting Research Base

Full-Time Equivalent (FTE) Researchers



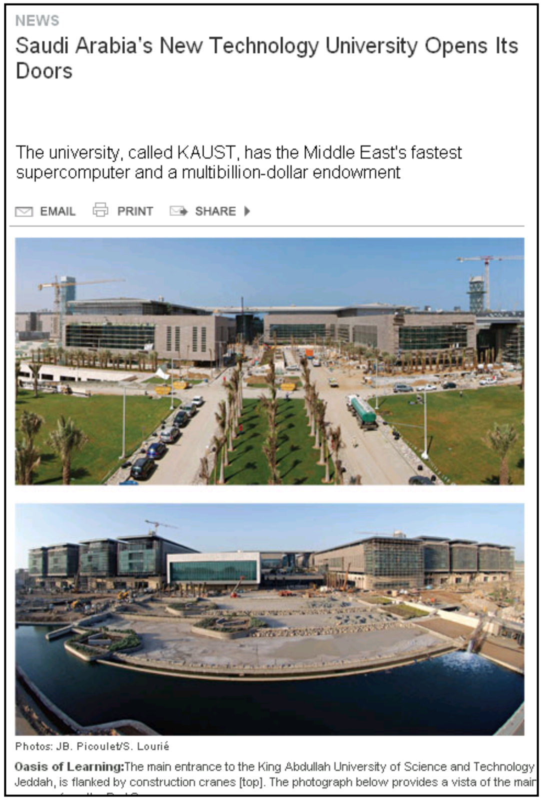
Source: OECD Science, Technology and Industry Outlook (2006)

Global Competition is Attracting U.S. Talent

- **KAUST (King Abdullah University of Science and Technology) -** IEEE Spectrum – September 2009

- **CSTDC (China Science and Technology Exchange Center) – September 2009**

- **CITDC (China International Talent Development Center)**

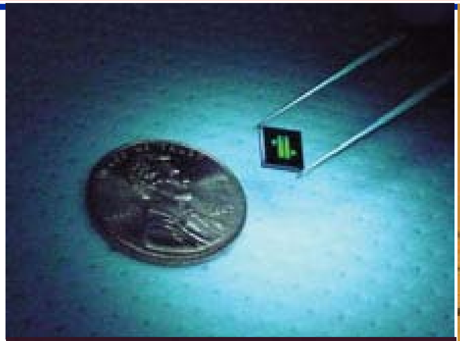


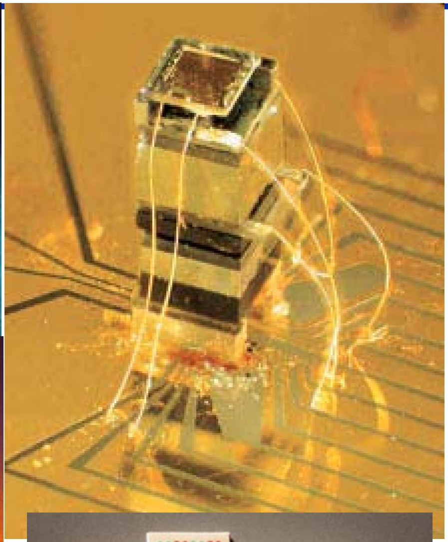
Where Will These Technologies Lead?

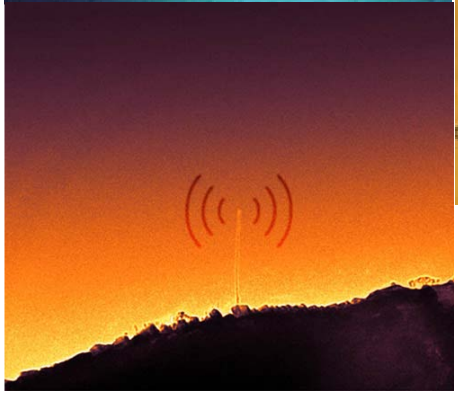
Science Becoming Global, Multidisciplinary

2009 MIT Innovations List of Top 10 Emerging Technologies:

- *Biological Machines*
- *Traveling Wave Reactor*
- *Racetrack Memory*
- *$100 Genome*
- *Software Defined Networking*
- *Intelligent Software Assistance*
- *Liquid Battery*
- *HashCache*
- *Nanopiezotronics*
- *Paper Diagnostic Tests*
- *Nanoradios (2008 holdover)*







Technology opportunities are expanding, but not well understood…

Prepare for an Uncertain Future – Do we have it right ?

- **Combating Weapons of Mass Destruction**
- **Advanced Tagging, Tracking, & Locating**
- **Cyberspace Operation/Protection Technologies**
- **Battlespace Awareness**
- **Energy & Power**
- **Unmanned Vehicles**
- **Advanced Electronics**
- **Advanced Materials**
- **Processing Large Data Sets**
- **Intelligence, Surveillance & Reconnaissance**
- **Human, Social, Cultural, Behavior Modeling**
- **Software Development**

Final Thoughts

Innovation

Speed

Agility

THE SPEED OF WAR

Improving the Speed and Cost of Turning Fleet Requirements into Fleet Capability

Michael McCrave
Alion Science & Technology
14 Oct 2009
mmccrave@alionscience.com
703-692-3288

Leadership: "The Speed of War"

" Our enemies…are well-funded, agile…and seek the most dangerous weapons."

*" We have seen the power and speed with which actions, images and ideas impact military operations. This **pace of change continually redefines the security environment** in which we operate."*

" We must follow through— rapidly execute — on every plan, budget decision, strategy and policy…to better defend…our national interests."

ADM Mullen as CNO in 2007
Chairman JCS

"Today on the battlefield, the IED fight, every 30 days, its competitive edge has changed. In the cyber-warfare fight, it's about every 14 days we change the competitive edge. You have to build an architecture, because everything can't be produced in 14 days or 30 days, " Cartwright said. "But you have to build it with the idea in mind that the unknown guy gets a vote. And a lot of times that unknown guy now has the throw weight to really do you in."

GEN Cartwright Vice CJCS 2009

Are we organized to outpace our adversaries?

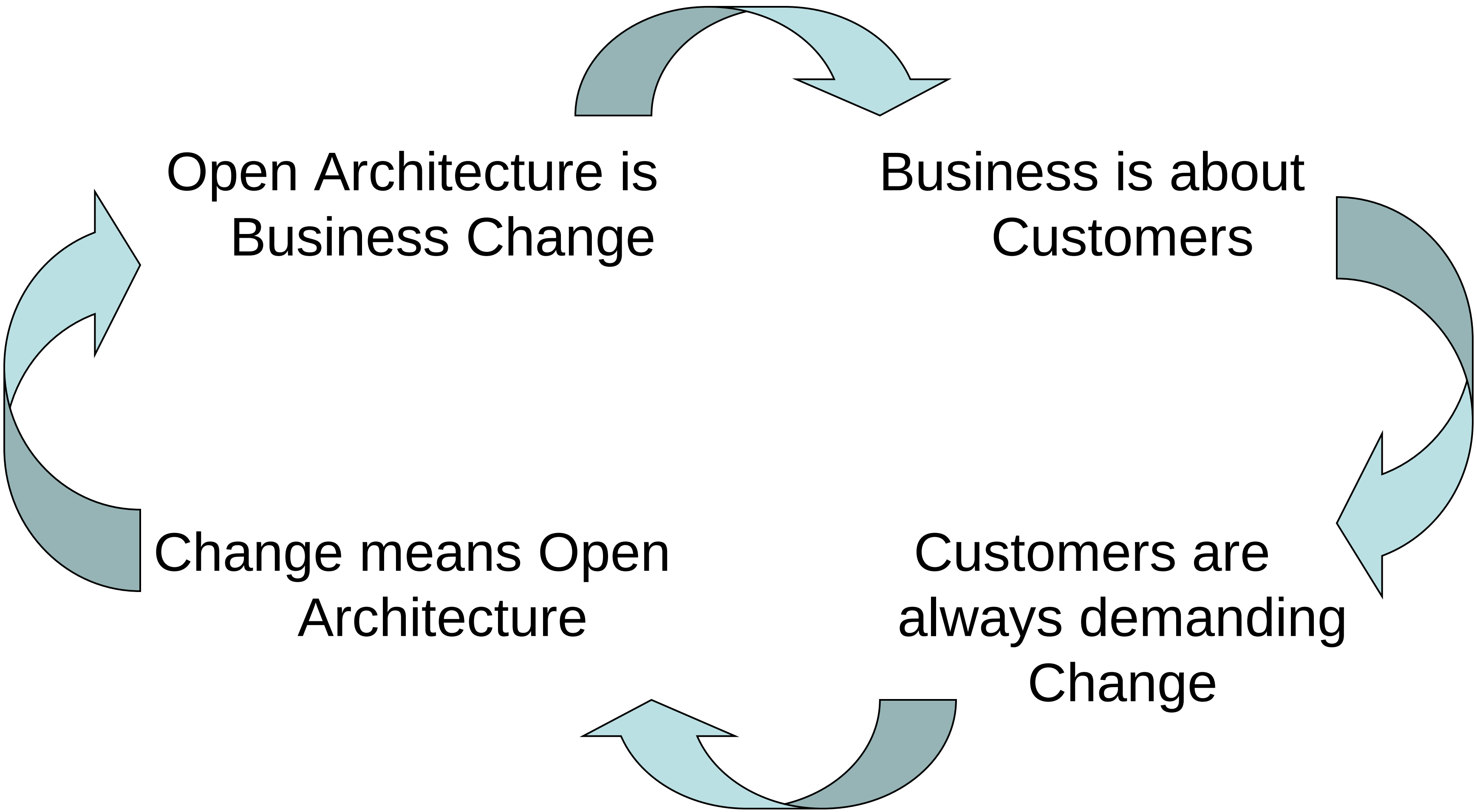
One Adversary… One Attack

"We bled Russia for ten years until it went bankrupt and was forced to withdraw in defeat. We are continuing the same policy to make America bleed profusely to the point of bankruptcy…

Al Qaeda spent $500K to carry out the attacks of September 11th, which caused America to spend more than $500B. Every dollar of Al Qaeda defeated $1M of America."

Osama Bin Laden, Oct 2004

Assumptions

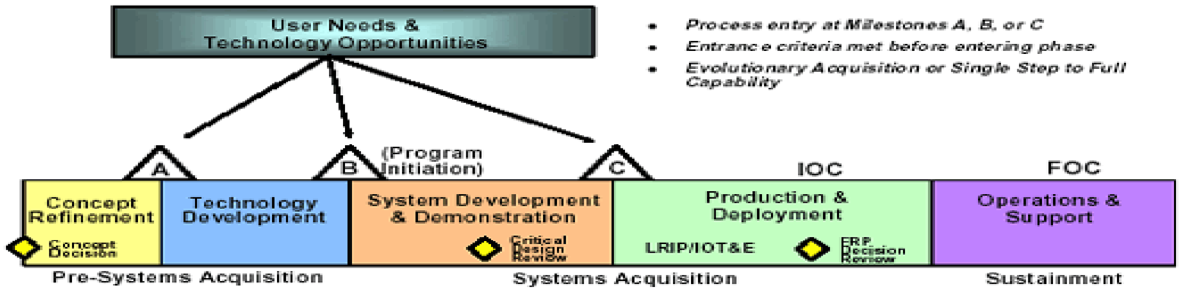


Commander's Guidance

- ***ALIGNMENT to deliver:***
  - *Right Capability – To fleet, not just new platforms*
  - *Right Time – Not "usual time plus fixes"*
  - *Right Cost – Not "usual cost plus inflation"*

- ***Enablers for Open Business Model:***
  - *Contracting Officials – Contracts drive the business*
  - *Cost Estimators – New cost models for modern techniques / business relationships*
  - *Test & Evaluation – New tools, new methods, single up processes*

OA changes business process



Business Changes

- Negotiate Data Rights to reuse components
- Disclosing designs to increase competition
- Structure contracts to include OA requirements
- Disclosing designs to increase competition
- Compete out components to drive innovation
- Reusing Components to drive down costs

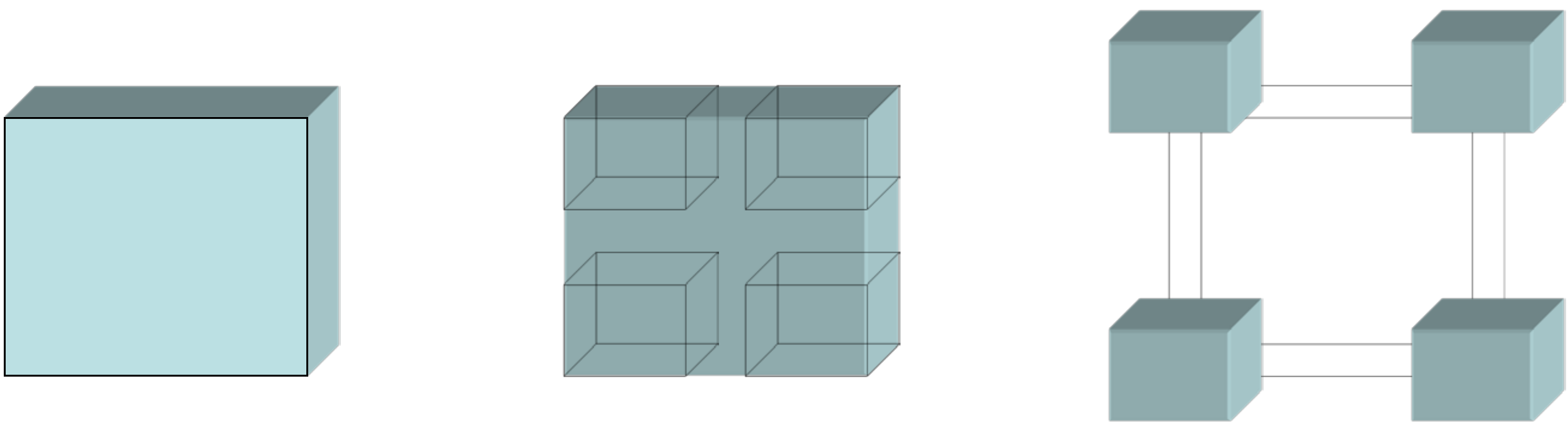
Technical Changes

- Modularize Systems to rapidly change components
- Define common services
- Define and publish key interfaces
- Design for adaptability
- Use open standards
- Automate testing

OA changes the way we design, build and support our systems

Degrees of OA transformation

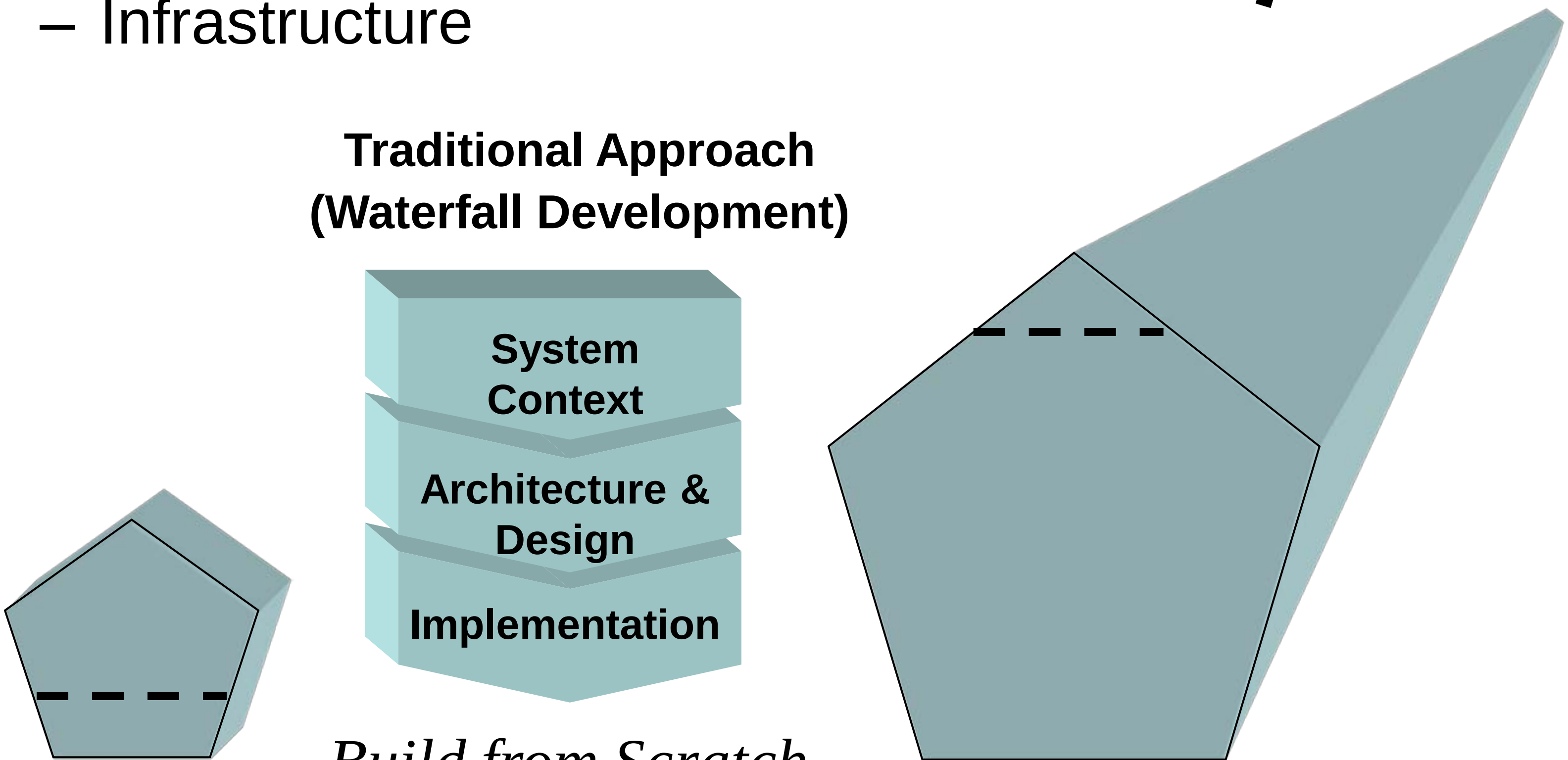
- How much “OA” – Business Model exposure risk
  - To competition
  - To innovation



“AS – IS” **“TO – BE”**

Darwinism?

- Survival of the Fittest…Open Anarchy?
- IP
  - Innovation
  - Infrastructure



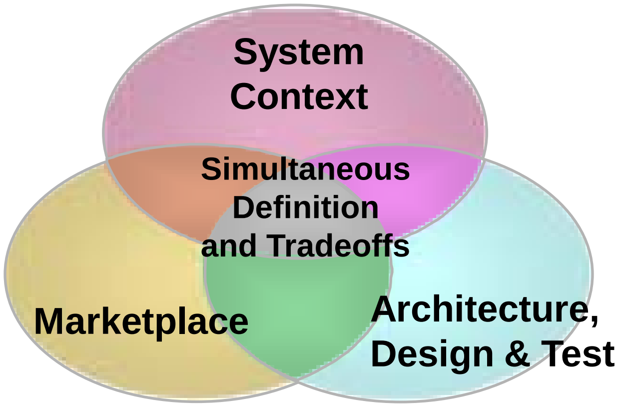
Build from Scratch

Source: Air Force COTS Study

Surviving Change

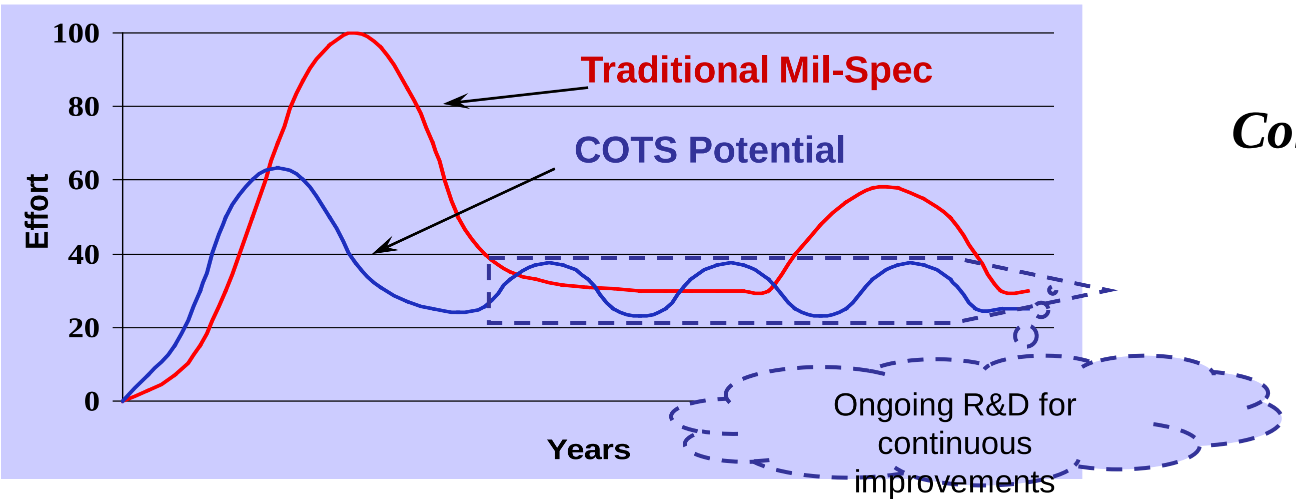
- **Change happens**
  - Change is both Risk & Opportunity
- **Cultural Shift**
- **Creative Destruction**
  - Innovation
  - IP

Open Architecture Approach (Spiral Development)



Buy, Integrate, Continuously Refresh

Notional Program Life-Cycle



OA Take-away

- **Opportunity to Accelerate**
  - Innovation
  - Cost-effective
  - Market share
- **Time is the threat**
  - Linear
  - Cyclic
  - Marketplace

"War is the great teacher of innovation, the great stimulus to thought in military affairs," says Ashton Carter, USD AT&L. The present wars, he adds, "have challenged the cultures in all the services… There's a heated competition to be relevant."

QUESTIONS?

Michael McCrave
Alion Science & Technology
14 Oct 2009
mmccrave@alionscience.com
703-692-3288

Open Computing System Definition

<u>Open computing system:</u> A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered components to be utilized across a wide range of systems with minimal changes, to interoperate with other components on local and remote systems, and to interact with users in a style that facilitates portability.

— Open Systems Joint Task Force

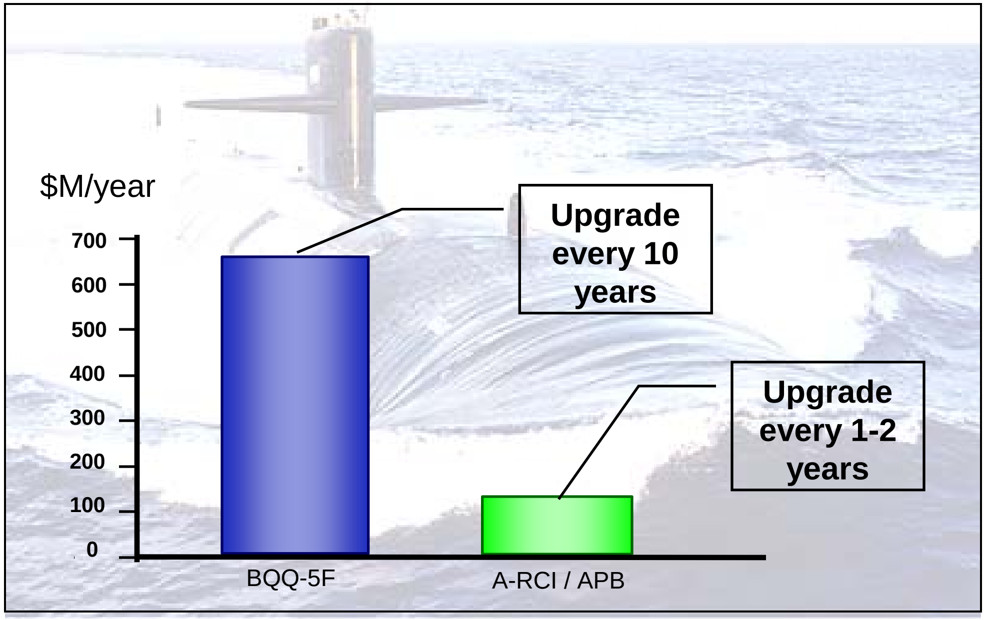
<u>Key Open Computing System Characteristics:</u>

- Based on open, publicly available specifications — preferably maintained as standards by a consensus process, e.g. by an internationally recognized governing group
- Well-defined, widely used non-proprietary (standard) interfaces, services and formats
- Durable (stable or slowly evolving) component interfaces that facilitate modular component replacement and addition of new capabilities
- Upgradeable through incorporation of additional or more capable modular components with minimal impact on the system

Open System Cost vs. Capability

- **PEO Subs competed or assigned system sub-divisions and gained significant cost savings - while rapidly increasing capability.**

Ten Year Comparison Development, Installation & Support Cost



"We refresh the hardware and upgrade software to continually improve capability and greatly reduce the amount of maintenance required by our Sailors. This business model, because of the regular tech insertions and APBs, allows us to rapidly introduce new capabilities into the fleet through an open architecture."
PEO Subs, June 2009

Open Business reduces infrastructure and total ownership costs while increasing capability

THE REVOLUTIONARY AND AWARD WINNING CYCLONE ENGINE – A TREMENDOUSLY PROMISING DISRUPTIVE TECHNOLOGY

Presented on 14 October 2009 at the Sixth Annual Disruptive Technologies Conference, by Dr. Phillip F. Myers, President – Advent Power Systems, Inc.

WHAT IS A DISRUPTIVE TECHNOLOGY?

- Usually a new paradigm – requires a new thought process
- Unconventional, novel, new, different
- Changes the way things are done and perceived
- Presents new and different possibilities
- May directly replace existing technologies
- Presents both an opportunity and a threat to existing organizations

SOME HISTORICAL PERSPECTIVES

- Integrated Circuits
  - $1 million in Air Force Funding to Texas Instruments - 1959
  - ICs absolutely necessary for all modern war-fighting
  - Generated more than $1 trillion in military and civilian procurement
  - A fundamental basis for US war-fighting dominance

MORE HISTORY - WORLD WAR II AND FUEL

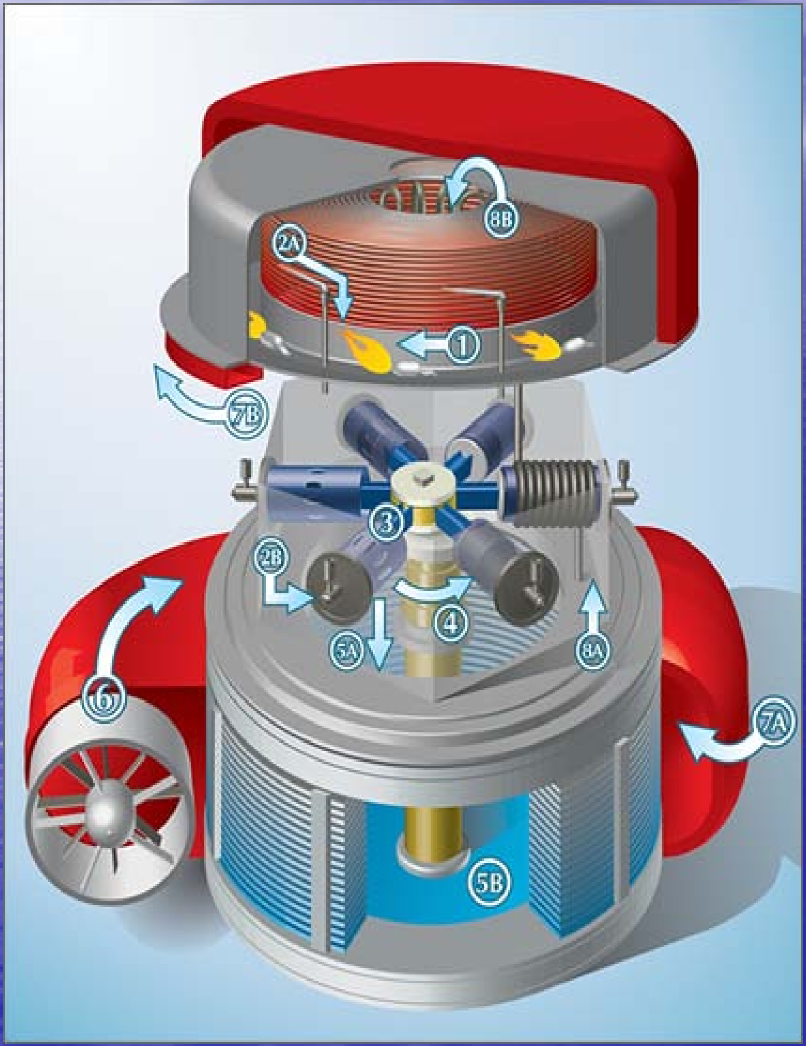
- Fuel availability was a central war consideration
- Japan claimed it went to war because it would soon run out of oil after U.S. embargo
- After strategic bombing of German oil resources at Ploesti and elsewhere the Wehrmacht and Luftwaffe ground to a halt
- Patton ran out of fuel on his advance across Europe
- Fuel cost and availability still critical issues
- A national priority is reduction of imported oil
- The Cyclone engine technology is a game changer, because it is broadly multi-fuel.
- With a Cyclone engine can use whatever local fuel is available, without regard to quality

WHAT IS THE CYCLONE TECHNOLOGY?

- Super high tech steam engine
- External combustion for complete clean fuel burning
- Heavily patented in US and overseas
- Engine validated by personal vetting of over 70 engineers and scientists:

“**There is no reason why it should not work. It obviously does work. It does not remotely push any laws of physics or thermodynamics. It is a simply brilliant invention.**”

THE INNOVATIVE CYCLONE TECHNOLOGY



HEAT PROCESS

(1) Fuel is atomized and injected into the patented centrifugal combustion chamber where a spark ignites the fuel-air mixture into a flame that spins around the heat coils. Thermocouples control the duration of combustion to keep the heat in the combustion chamber at a constant temperature. **(2A)** Water contained in the coils becomes super-heated steam (up to 1200°F) which is piped to the cylinders, **(2B)** where it enters through a patent-pending valve system (not pictured).

MECHANICAL PROCESS

(3) Steam enters the six radial-configured cylinders under pressures up to 3200 psi to push the pistons in sequence. Note, no motor oil is used – water is both the working fluid and engine lubricant. Also, because of the valve design, the engine starts without the need of a starter motor. **(4)** The rotating action of the pistons connected through a patent-pending spider bearing (not pictured) turns the crank shaft. Note, because the greatest amount of torque occurs at the first rotation, the shaft can be directly connected to a drive train without a transmission.

COOLING PROCESS

(5A) Steam escapes the cylinders through exhaust ports and enters the patent-pending condensing unit where it turns back into water, and **(5B)** collects in a sealed pan at the bottom of the condenser. Note, this is a closed-loop system – the water does not need to be replaced or topped-off. **(6)** Blowers spin fresh air around the condenser to speed the cooling process.

REGENERATIVE PROCESS

(7A) Air which has been pre-heated from the condensing unit, **(7B)** continues up to a second heat exchanger located in the exhaust port of the combustion chamber, further pre-heating the air used for combustion while also cooling the exhaust fumes (to about 320°F). **(8A)** A high pressure pump (not pictured) pipes water from the collecting pan to the heat coils via heat exchangers surrounding each of the cylinders (only one pictured), and then **(8B)** to the center of the coils to start the heat cycle again.

CYCLONE ENGINE CHARACTERISTICS

- External combustion – clean burning, efficient
- Water lubricated, closed system
- Burns any fuel – JP5 OR 8, Diesel, dirty Diesel, bio-diesel, gasoline, alcohol, algae fuel, orange peels, garbage, biomass, powdered coal
- Operates like the most modern steam power plants
- Typical operating temps of 1200 F, and 3,200 psi
- Quiet, low vibration, low IR signature
- High thermal efficiencies – 30% now, up to 40% later
- Lite weight and compact - ~ half the volume and weight of a full Diesel system.
- Very high torque – 7+ foot pounds/horsepower @ 1 rpm
- Almost invulnerable to IEDs, shrapnel, or small arms fire

THE "MISSING ENGINE"

- The Cyclone Engine is missing all the following components/systems and has:

-No sophisticated fuel injection system

-No sophisticated spark ignition system

-No high pressure fuel pump

-No oil, oil pump, oil pan

-No external radiator, hoses, water pump, coolant, or fan

-No catalytic combustor

-No transmission

LAND BASED MILITARY APPLICATIONS

SOME OF THE MANY MILITARY APPLICATIONS

ABRAMS MAIN BATTLE TANK

STRYKER ARMORED VEHICLE

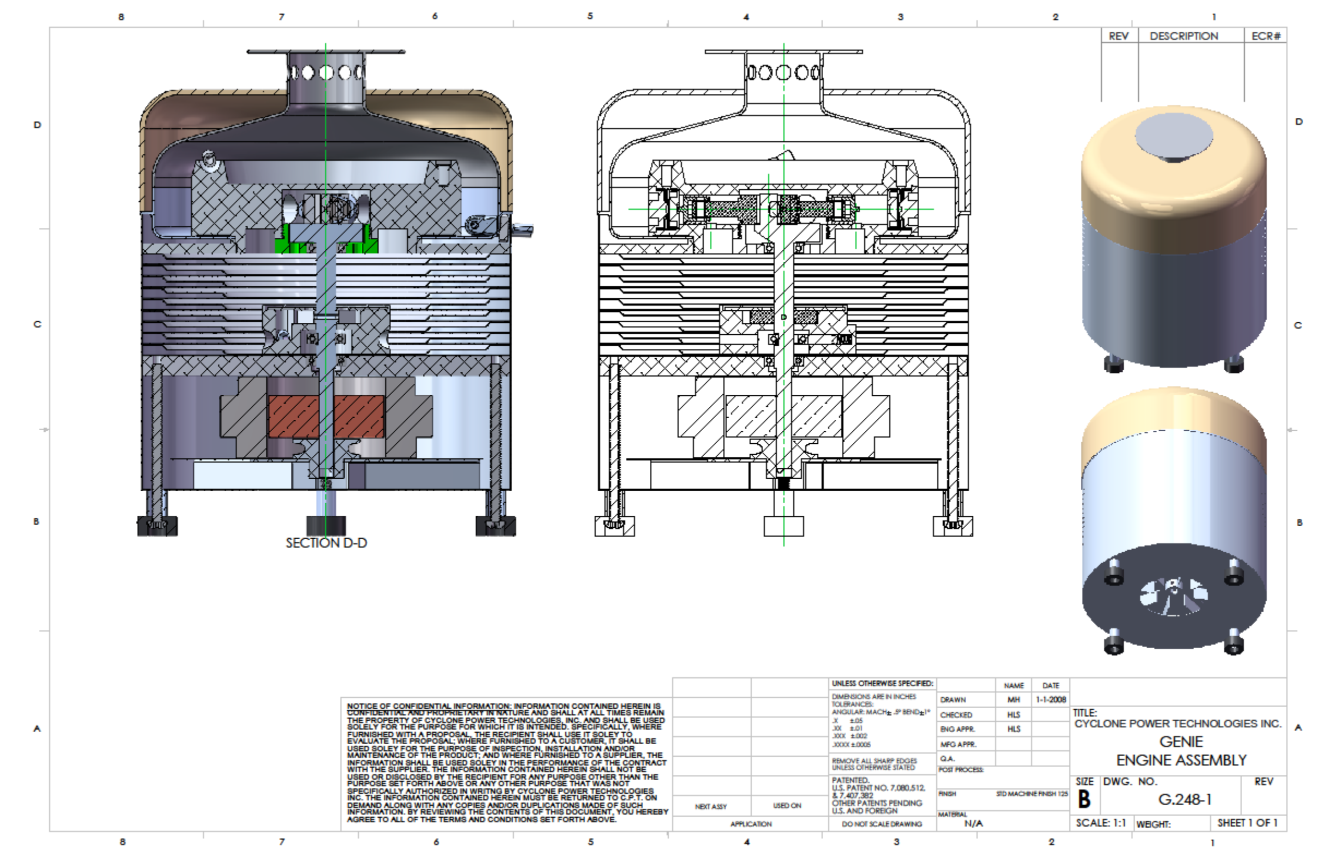
HUMVEE

CYCLONE APU

LAND APPLICATIONS

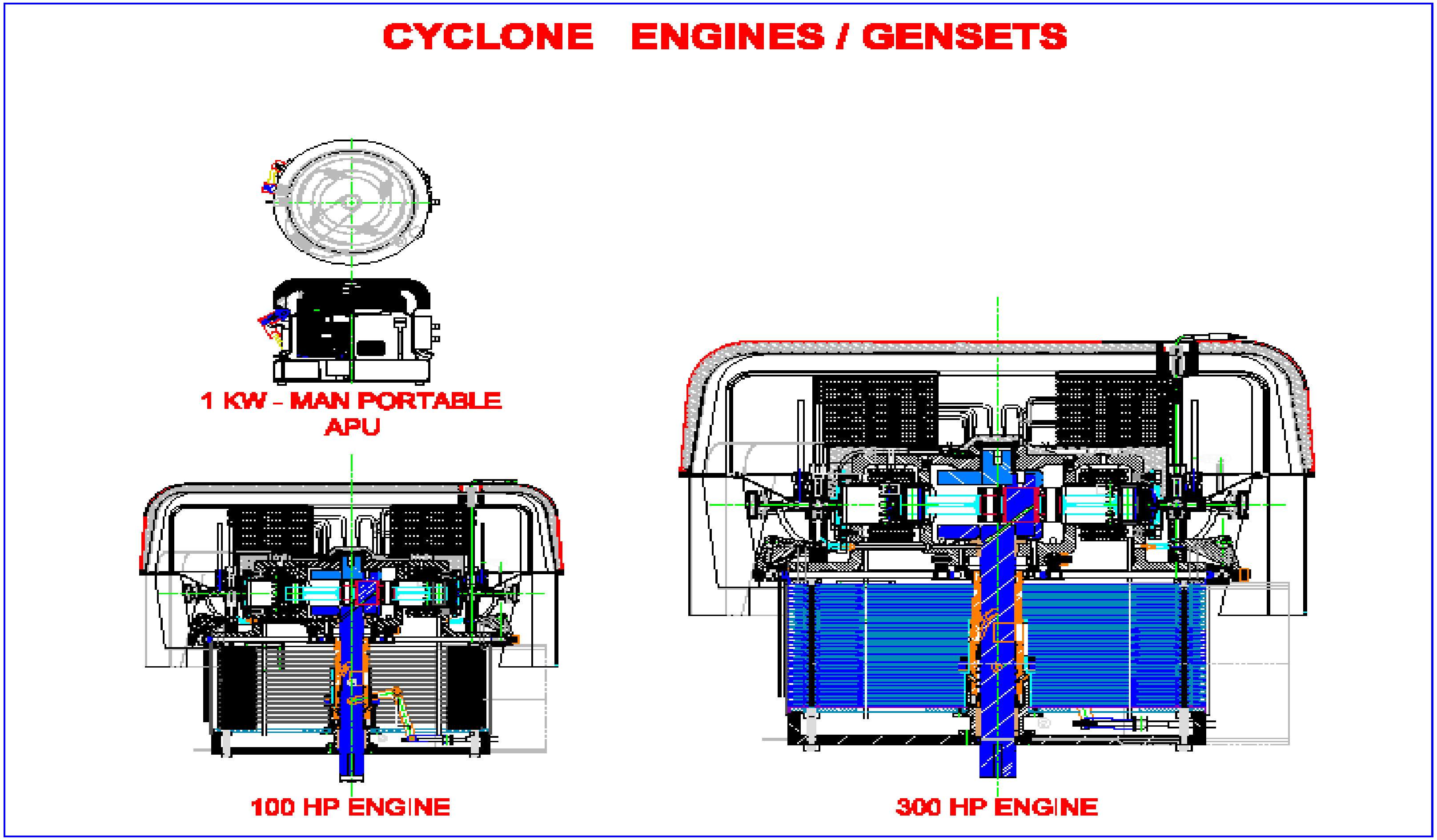
- Drive engines for tanks, HUMVEES, trucks
- Auxiliary power units for these vehicles
- Gensets – 1 to 1,000 kilowatts
- Power source for hybrid electric vehicles
- Small man portable units-80 to 1,000 watts (tremendous cost savings/logistic support ease over batteries) for field use/special forces
- Autonomous ground vehicles

GENIE 80 TO 200 WATT MAN-PORTABLE POWER PLANT



ROBOTIC APPLICATIONS

FROM SMALL TO LARGE CYCLONE ENGINES



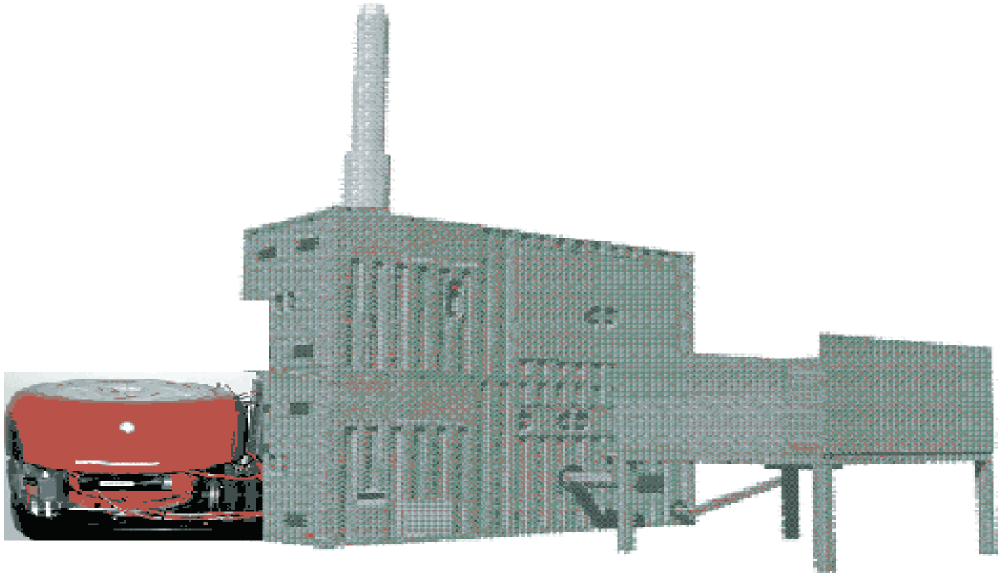
NAVAL AND AIR APPLICATIONS

- Naval Applications:
- Drive motors for boats and ships
- APUs for boats and ships
- New engines for torpedoes
- Engines for underwater craft, manned and unmanned
- Bottom dwelling weapons platforms
- Air Applications:
- UAVs and UCAVs

FIXED BASE APPLICATIONS

- To burn garbage and generate power
- To run on algae fuel for base power
- To run on other available biomass
- To substantially reduce costs
- To provide local energy independence

DIRECT COMBUSTION OF BIOMASS TO PRODUCE ELECTRICITY



BIOMASS FUELED ELECTRIC POWER GENERATOR

SO WHY IS THIS A GAME CHANGER?

- Can drastically improve fuel logistics in combat or forward base areas since Cyclone engines will burn practically anything
- Huge cost savings-burning algae fuel or other biomass
- Savings on repairs, maintenance, parts
- Greater flexibility of vehicle design
- Drastic reduction in vehicle vulnerability, because no external radiators (3 minute rule)

WHERE ARE WE AND WHAT DO WE NEED?

- Working with five of ten largest defense contractors
- Raytheon has been publicly named
- Developing a variety of engines, mostly on private funds
- Badly need military funding to accelerate pace and range of engine development
- Military applications should lead to major cost savings from fuel logistics and lower cost fuels
- Spinoff to private sector will generate large tax revenues, as in integrated circuit case.

APS SENIOR MANAGEMENT

- Dr. Phillip F. Myers – Founder, President, CEO – BIE, MBA – Ohio State, Doctorate – Harvard Business School. 30+ years business/management experience, in small, medium, and large companies. Formed 12 new companies. Extensive consulting, teaching, public service experience. Former Air Force Captain, Engineering Officer, and War Planner
- Allyn Armstrong – Sr. V.P. – Chemical Engr, Executive M.B.A. – Ohio State. Heavy consulting + management experience.
- Steve Lebishak – Coast Guard Academy, MIT, Wharton – V.P.-Finance
- Rich Belaire – Retired Ford Superstar Engine Engineer
- Brij Bhargava – One of top generator designers in world

CONTACT INFORMATION

- Dr. Phillip F. Myers, President
- Advent Power Systems, Inc.
- (Veteran Owned Small Business)
- 2904 Victoria Place, Suite C2
- Coconut Creek, Florida 33066
- Phone: 954-979-6510
- Fax: 954-977-4460
- E-Mail: philmyers@adventflorida.com
- Website: www.adventflorida.com

National Defense IndustrialAssociation

6th Annual Disruptive Technologies Conference

"SCIF Construction: Unraveling The Mystery"

Jason Phillippe, Director
Intelligence Programs and Operations
Copper River Information Technology

Joseph Cooper, President
SCIF Constructors, LLC

History of ICD 705

- National Intelligence Strategy “Uniformity and Reciprocity”
- Formation and involvement of the Physical and Technical Security Working Group (PTSEWG)
- New policy structure (ICD’s, ICPG’s, ICPM’s and ICS)
- Changes and challenges of ICD 705

- Significant Policy changes from DCID 6/9 to ICD 705
  - Additional new labor categories (Site Security Manager, Construction Security Technician, Admin Support)
  - Emergency Plans and Required SCIF Document Storage
  - Defined "Security in Depth"
  - No more "SCIF within a SCIF" with "Compartmented Areas"….etc….

- Significant Construction Change Requirements
  - Specifies precisely how to build a SCIF wall
    - *Includes* detailed diagrams
  - 16 gauge steel studs 16 inches on center
  - ¾ inch pressure treated plywood on “enhanced walls”
  - Allows use of SCIF Clips vs welding for 9 gauge install

- The new paradigm for SCIF construction and associated costs….
  - Industry cost study by ISWG
  - Average SCIF Cost 24.2% higher
  - New clearance requirements in SCIF construction
  - SSM requires TS/SCI
  - Alarm maintenance techs require TS/SCI
  - Timeline for new policy implementation
  - Impact and implementation

LOCKHEED MARTIN

Counterspace Capabilities using Small Satellites: Bridging the Gap in Space Situational Awareness

6TH ANNUAL DISRUPTIVE TECHNOLOGIES CONFERENCE
Washington, DC

October 14, 2009

Rick Mullikin
Lockheed Martin
Information Systems and Global Services

Introduction

- A great deal of work has been done recently with regard to smallsats
  - Also known as microsats, minisats, nanosats, picosats and cubesats.
- The low cost and rapid insertion into space is changing the face of the way we view satellites
  - Innovations in manufacturing, miniaturization and fabrication quality have made the concept of smaller, lighter and lower-cost satellites that perform mission critical functions a possibility.
  - Until recently, their development has remained mostly an academic practice advanced by universities and small research outfits, but this is changing.
- With these advancements also comes a threat.
- To date, at least 30 countries have operated microsatellites
  - China recently established the “world’s largest microsatellite industry park.”

The Threat

- Advances in miniaturization and proliferation of space technology will provide rogue nations access to very small anti-satellite systems
  - Geopolitical drivers provide the motivation for countering the sovereignty of the United States in space.

- Small satellites have lowered the cost of entry into the once elite space club, thus allowing nontraditional countries to become players

- This openness to space also creates a new threat from hostile nations

- With access to the exact same technological breakthroughs, our nation’s satellites become exposed to unmonitored attacks, crippling national security

Capability Gap

One example: Results of a recent Air Force Space Command War Games assessment (Schriever War Games 5):

Conclusion:

"an enemy with more advanced space assets can disable U.S. force capabilities, largely through the use of small satellites which cannot be tracked, monitored, or assessed."

AIR FORCE SPACE COMMAND

- General C. Robert Kehler
- Lt. Gen. Larry James
USAF 14th Air Wing

Example of U.S. shortfall, sensors weren't able to pick up eight small satellites launched by the Japanese earlier this year until after they flew over the South Pole through the U.S. sensor network. This is the same problem U.S. commanders face with launches from China.

LOCKHEED MARTIN

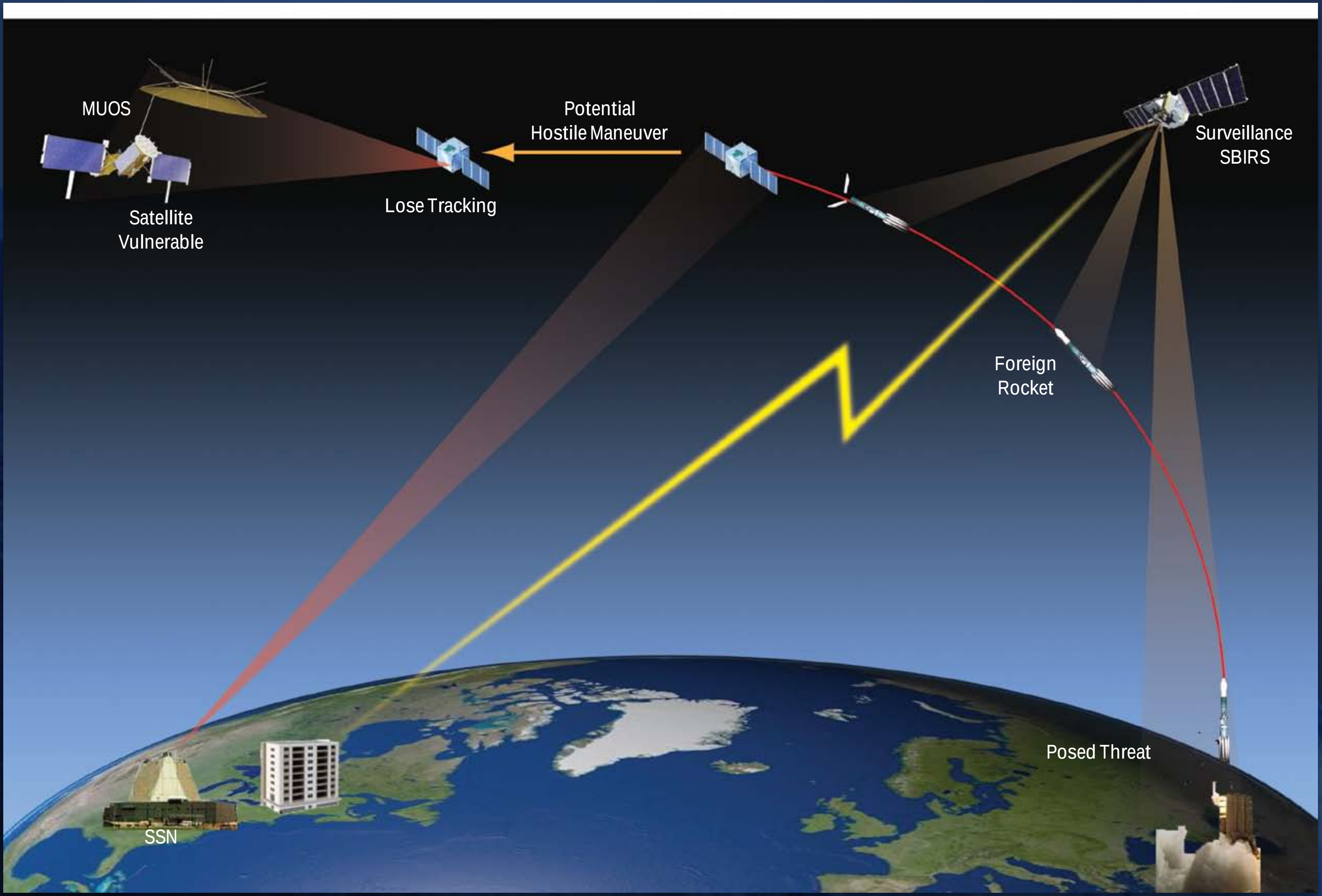
Hypothetical Scenario (AS-IS)

What looks like a typical comm satellite is launched and placed in orbit

Later, undetectable swarm of smallsats deploy in vicinity of a U.S. asset

U.S. asset is disabled- all comms are lost

10 years from today



Hypothetical Scenario - Details

Time	Location	Operation
0915Z 11 Jul 2019	Somewhere in the Pacific Ocean	The USS Ronald Reagan loses its satellite communications (SATCOM) link to Headquarters, U.S. Pacific Fleet. Nearby, a nuclear attack submarine surfaces to make contact with headquarters during its designated reporting window, but is unable to acquire its SATCOM link. The sub commander directs the communications officer to try again using the alternate link.
0917Z	Joint Space Operations Center (JSpOC), Vandenberg AFB, CA	The Senior Space Duty Officer (SSDO) is notified that the Advanced Extremely High Frequency (EHF-4) has entered safehold mode after experiencing an unknown anomaly. The space weather officer reports that solar activity is high so the satellite may have experienced a "single event upset" due to solar radiation. The SSDO requests an update on the situation in 10 minutes.
0919Z	JSpOC, Vandenberg AFB, CA	The SSDO sees an alert on her Common Operating Picture display indicating that U.S. Pacific Fleet is experiencing communications problems. As she reads the alert, she receives a call from the watch officer at the Wing Integrated Operations Center (WIOC) at Schriever AFB. The WIOC watch officer reports that the 50th Space Wing has lost contact with the Mobile User Objective System 5 (MUOS-5) satellite. Prior to losing contact, all systems were within normal operating limits; however, the satellite is aging and well past its design life and this isn't the first time they've had problems with bird 5. The WIOC watch officer reports that MUOS-5 had been servicing U.S. Pacific Fleet.
6 Months Earlier	Jiuquan Space Facility, China	A Long March 6 rocket lifts off carrying the Indonesian IndoCom-7C communications satellite. The satellite is placed into geosynchronous orbit (GEO) to provide wideband communications. The U.S. Space Surveillance Network (SSN) observes the launch, and within minutes, the Space Based Space Surveillance (SBSS) system computes the IndoCom-7C orbit and verifies that it has been placed into the pre-announced orbital slot. SBSS continues to watch as IndoCom-7C completes its deployment maneuvers and unfurls its solar arrays. After verifying that the IndoCom launch appears nominal, SBSS-2B is re-tasked.
Fast forward to 1 Jul, 2019 2034Z	22,000 miles above the earth, somewhere over the Pacific	What looks like a radiator panel on the side of IndoCom-7C swings open. Thirty-two cubes, each about 10 centimeters across, fly out of the IndoCom opening. This event is not detected by the SSN. The cubes automatically configure themselves into an autonomous cluster and silently navigate to their destination.
11 Jul, 2019	Near MUOS-5 satellite	A swarm of miniature satellites, operating as a virtual cluster, approach the MUOS-5 spacecraft. Undetected by any U.S. system, the cluster identifies the main electrical panel onboard MUOS-5 and attacks. Seconds later, MUOS-5 powers off its transponders as the onboard computer malfunctions. Twenty-two thousand miles below, the USS Ronald Reagan loses its satellite communication link
	Over the Pacific Ocean	All U.S. military satellites previously operating over the Pacific Ocean are now inoperative, and all of Pacific Fleet is deaf.

Premise of Concept

1. Current space tracking systems will never be able to watch everything all the time, especially given the proliferation of small satellites

2. Even if this were possible, no current capability exists to discern between those with hostile intent

3. Further, there are no effective, existing, space-warfare simulations that adequately capture the emerging technologies in small-satellite development

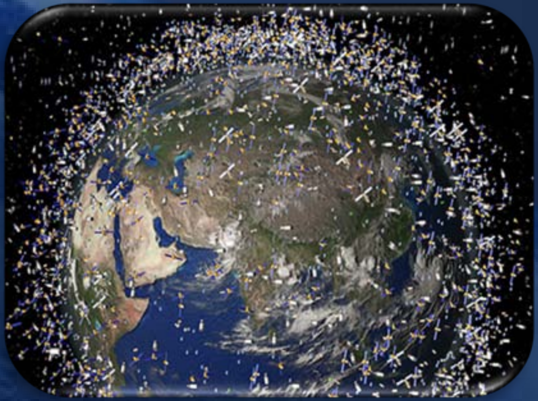
LOCKHEED MARTIN

Challenges

- **There is no methodology to model and simulate the system-of-systems needed to provide end-to-end situational awareness for complete traceability of a potentially hostile satellite back to its host country**

- **Any new methodology must also provide enough information to determine whether a satellite is active -- and its capabilities**

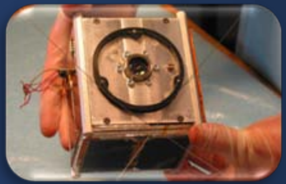
- **The solution must be able to maintain "knowledge custody" of all space objects from the moment of launch**
  - **if a hostile space attack occurs, the system can produce an "indisputable chain of evidence".**



LOCKHEED MARTIN

Why Smallsats as part of the solution?

- Quick response (i.e., able to load and launch more rapidly)
- Low-cost risk (smallsats are very inexpensive to build/test)
- Inherently invulnerable as a whole
- Wide range of surveillance
- Close proximity for ASAT observation and data gathering
- Highly maneuverable



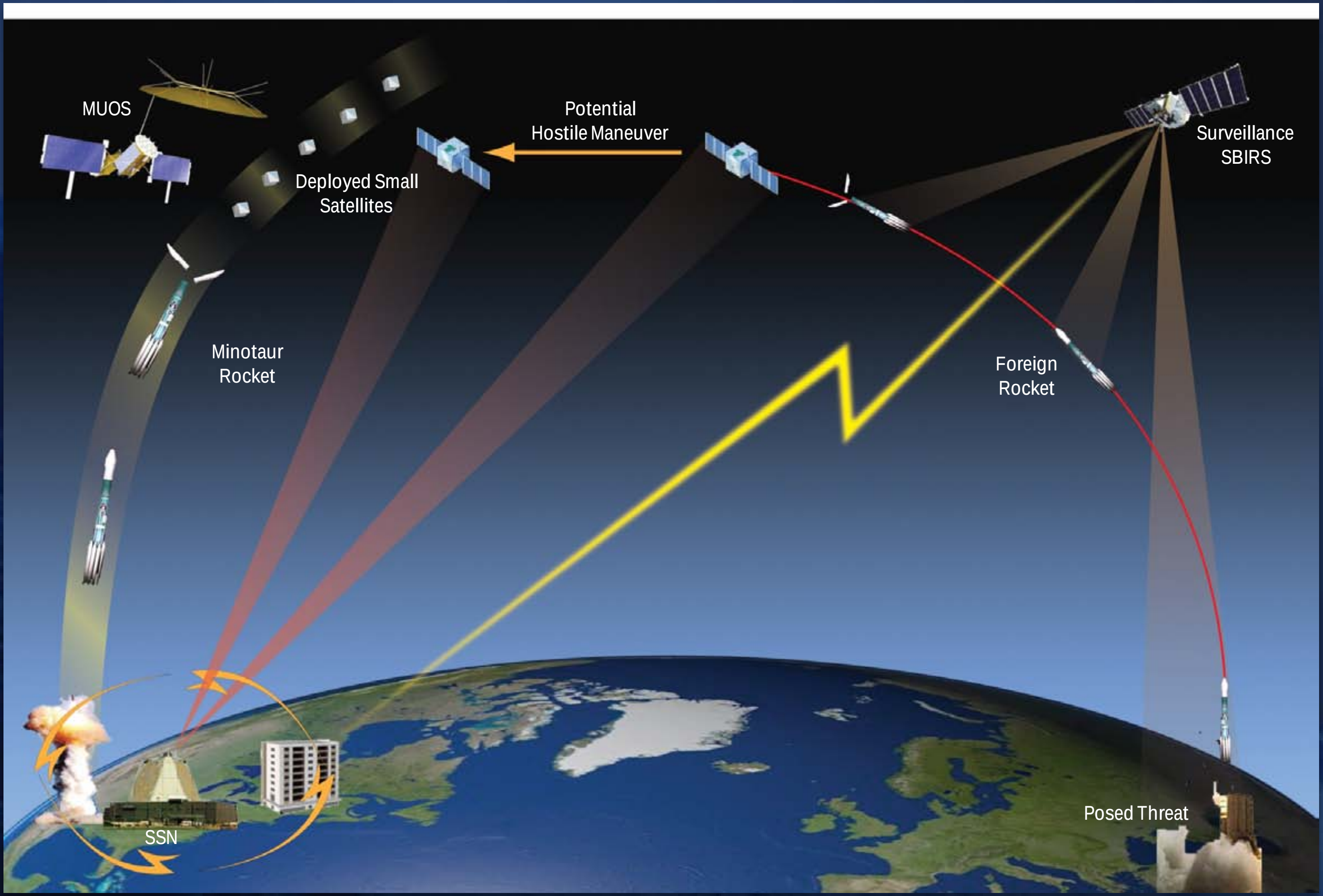
With small satellite capabilities emerging, the tools we have foster the ability to rapidly incorporate these new capabilities into the solution.

Envisioned Capability (TO-BE)

Through integration of several systems -coordinating these activities provides critical space situational awareness

Tracking ability of a potentially rogue vehicle back to its host country

Sufficient forewarning of a potential hostile attack, we can initiate the launch of small satellites in rapid fashion to likely prevent such an attack



Our Research So Far - Macro

TECHNOLOGY GOALS:

1) enabling technologies and methodologies, advanced concepts and algorithms, and artificial intelligence for protection against small satellites

2) advanced research into improving space situational awareness (SSA) given the threat of adversarial small satellites

Current work under way has led to the development of a series of predictive computer models

For example, for a set of mission objectives, the system will be able to tell the user the best fit (economics and performance) be it large, small, mini, micro, nano, pico, femto, or a constellation combination

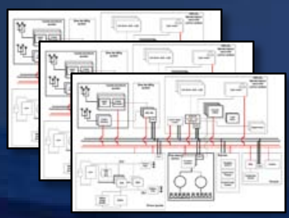
LOCKHEED MARTIN

Our Response - Micro

- As part of a systems-of-systems solution, develop and deliver a capability in the form of an analytical framework
- Make extensive use of advanced modeling and simulation tools and algorithms that capture the current surveillance architecture, as well as current and future satellite capabilities most importantly including small satellites
- This framework can then be leveraged to determine the best way to assess hostile intent and to protect our national—and commercial—assets
- The end result system will lead toward an “indisputable chain of evidence” leading to attribution

Initial Tools and Processes Used

Architectures



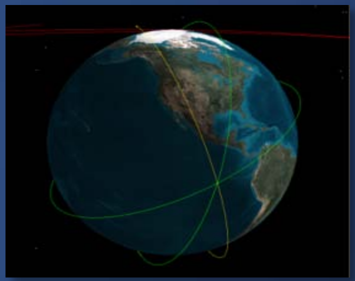
- *Space-Based Surveillance Systems*
- *Ground-Based Processing*
- *Small Satellite*

Scenarios

- *Major System Roles*
- *Small Satellite Roles*
  - *Observation and Data Gathering*
  - *Data Communication*
  - *Maneuvers*
  - *Offensive and/or Defensive Actions*

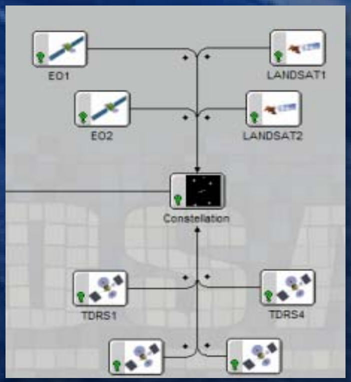
Driven by Real-World Architectures & Scenarios

Physical World Model and Visualization



- *Scenario Entities and Payloads*
- *Orbit Dynamics and Maneuvers*
- *Monte Carlo Simulation End-game*

Integrated using MOSAIC



- *Functional Flow Diagrams*
- *Decision Logic & HITL*
- *Tie Points to Physical Models*

Discrete Event Simulation

Other Technologies (Wild Possibilities)

Ladar / hyperspectral characterization of the micro sats

> determine their fingerprint so they can be recognized whenever they come and go through our net

> enabling detailed tracking and anomaly recognition (for example when orbit changes)

COMINT characterization of the satellites

> how often and with what density do they communicate, and with whom and where

> build models of the types of satellites based on their comm??

MASINT (if active sensors are on board)

Also Make Use of SSN/Space Fence

- Through modeling and simulation, a set of designs can be better integrated to provide the capability to track an asset from launch to de-orbit.
- Tracking of the launch to deployment via SSN is followed by the space asset until the launched vehicle is in its initial orbit
- Tracking could then be handed over to the formation of small satellites to get "close-up" pictures and other data from the potentially hostile satellite

	Current AFSSS	Space Fence System
Frequency	VHF	S-Band
Observations per Day	170,000	750,000
Catalog Size	Nearly 10,000 Objects	400,000 Objects
Radar Coverage	12,000 km Maximum ±90° E-W	250 km Minimum 22,000 km Maximum ±60° E-W
Object Detection	30 cm or Larger	5 cm or Larger
Detection Sensitivity	Classified	LEO: 95% Prob. Of Detect. MEO: 90% Prob. of Detect.

End Result - Operationally Speaking

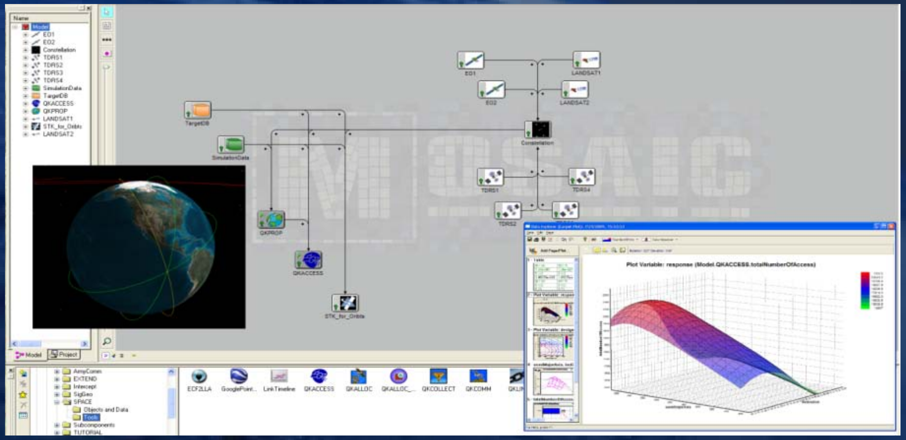
- Ability to track satellites from launch through to de-orbit, including any potentially hostile maneuvers
  - U.S. would be ready to act with fully informed decisions

- Quickly converge on what satellite(s) may be causing the problem in the vicinity of the lost communication satellite
  - traceability back to the host nation that launched the vehicle(s).

- With rapid deployment of a swarm of small satellites, (for example), we would be able to take near-real-time defensive or offensive action directly on the invasive hostile satellite(s)

Conclusion

- The threat of small satellites being used against the U.S. is real
- Not a matter of IF -- but WHEN
- Very little has been accomplished to date to have a solid retaliation plan
- The time is now to begin to develop truly innovative models that lead to real-world solutions



LOCKHEED MARTIN

Thank you for your time!

Further contact:

Dr. Rick Mullikin
rick.mullikin@lmco.com
Phone: 917-497-0424

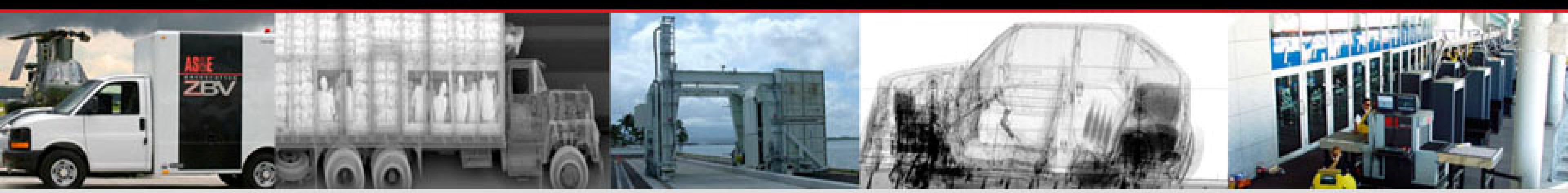
Miniaturized, Modular, High Resolution X-ray Backscatter Imaging as a Blue Force Enhancer

Bill Baukus
Director, Technology Development
October 14, 2009

6th Annual Disruptive Technologies Conference

AMERICAN SCIENCE AND ENGINEERING, INC.

AS&E



Distribution Statement A: Distribution Unlimited

This Presentation is Unclassified

Overview

- The Need
- X-ray Backscatter Imaging as a Disruptive Technology and Blue Force Enhancement
- Applications and Configurations
- Challenges/Observations

The Need: Maneuverable, Fast, High Resolution Threat Detection

Don’t let these events happen

X-ray Backscatter Today

- One-sided Inspection
  - VBIEDs
  - Drugs
  - Weapons
  - Other contraband
- Discriminates Lo Z and Hi Z
- Fast
- User Friendly
- Adaptable and Transportable

Backscatter Images Reveal A Variety of Contraband

Smaller, Lighter, Higher Resolution, Modular Systems Provide Additional Blue Force Enhancement

- **Current systems fill a valuable need**
- **Tomorrow's systems will provide additional capabilities for our forces**
  - **TSWG/NIJ: Trailer-mounted robot borne system**
  - **Army/RDECOM/I2WD: Miniaturized Imager**
  - **DHS/S&T: Modularized Backscatter**
- **Goals: Expand the flexibility, performance and application base for single-sided imaging**

Miniaturized Backscatter System – An Expandable, Adaptable Concept

AS&E

- Large system
- Objects at a distance

TSWG/NIJ Program

- Small system
- Objects up close
- Adaptable for standoff

Control Electronics

Data Collection

Heat Exchanger

Detectors

X-ray source
• X-ray tube

HVPS

Shielding

Control/Display
• Laptop

Main Power
• Wallplug
• Battery

Beam Forming Subsystem

Vertical Scan Mechanism
• Collimation Wheel

Horizontal Scan Mechanism
• Rotating Turret

Transport/Platform

Single-Sided Imaging Module
• Single Unit
or
• Modular Assembly

The First Prototype

<u>Prototype:</u>

Imager Weight 320 Pounds

Imager Size Width: 27.0”

Depth: 31.5”

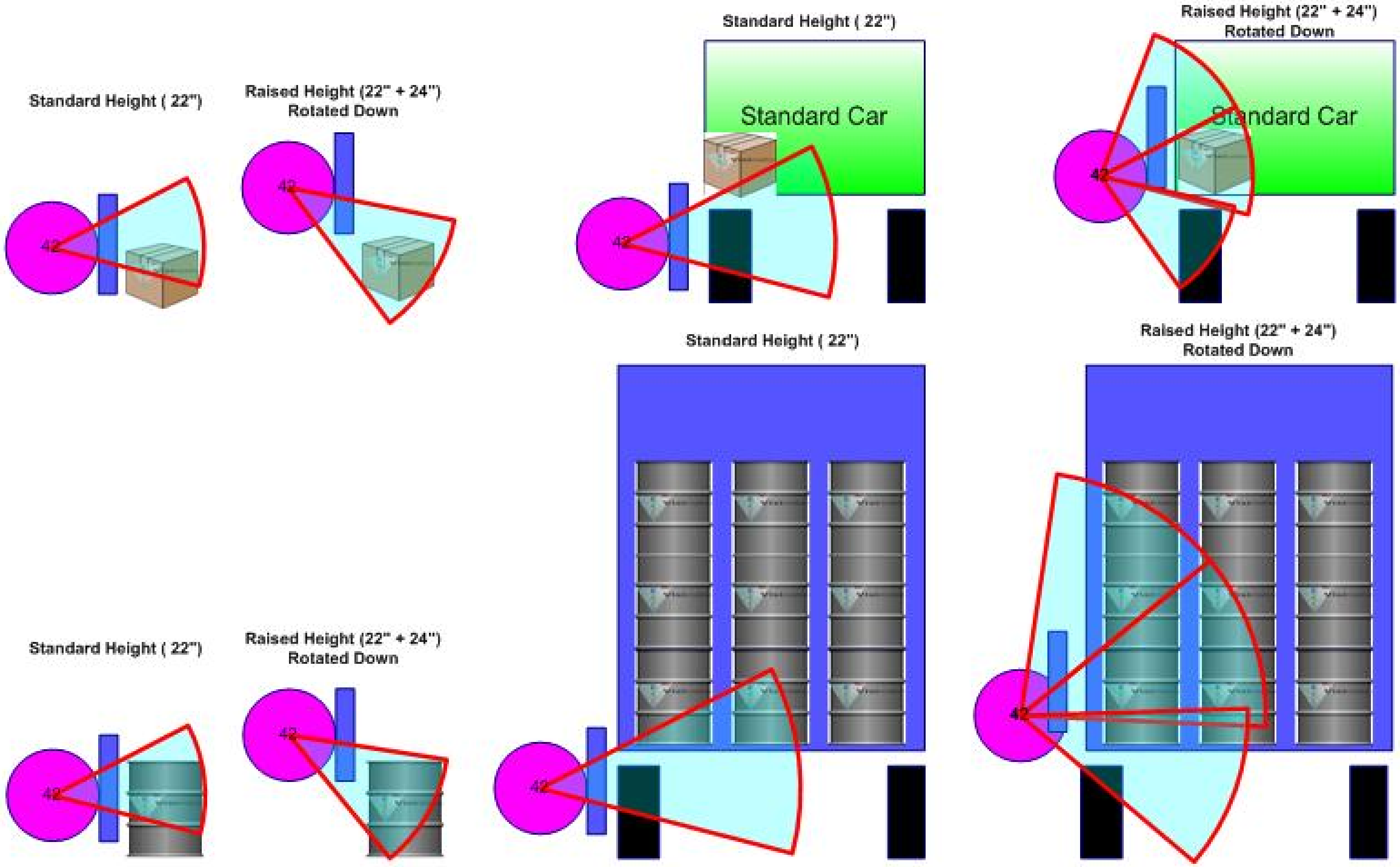
Height: 31.5”

Second Unit to be smaller and lighter

~ 250 pounds, 19.5” x 24.5” x 30”

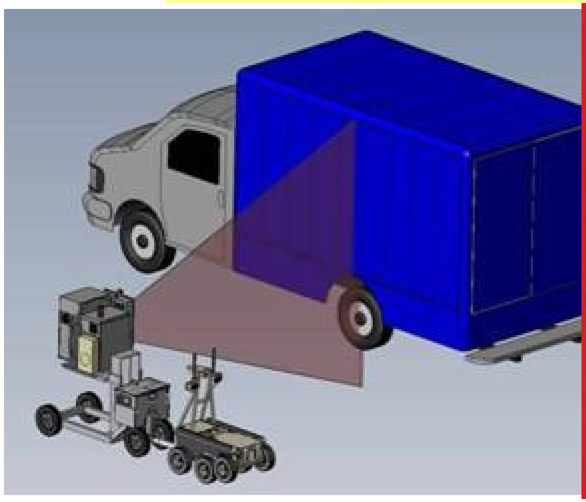
Variable Positioning Provides Flexibility

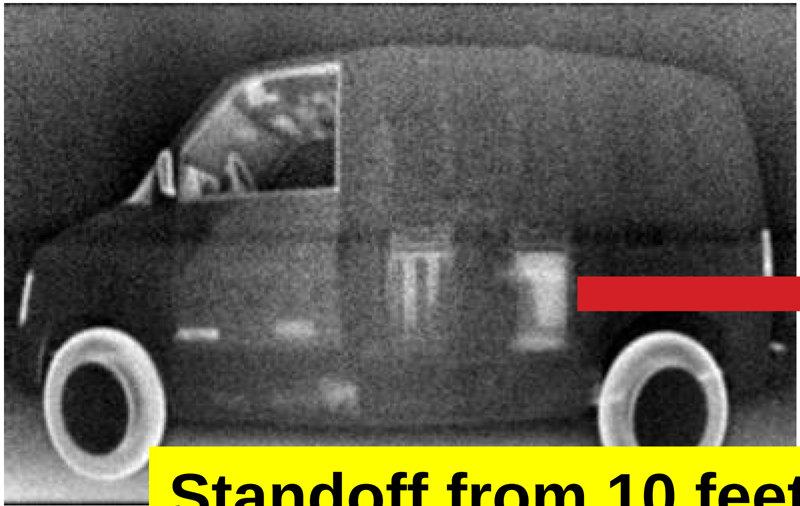
- **<u>Scanning Wheel X-Ray Angle Changes +/- 30 Degrees</u>**
- **<u>Detector Set Raises and Lowers as needed from 22 - 25” Nominal Scanning height</u>**



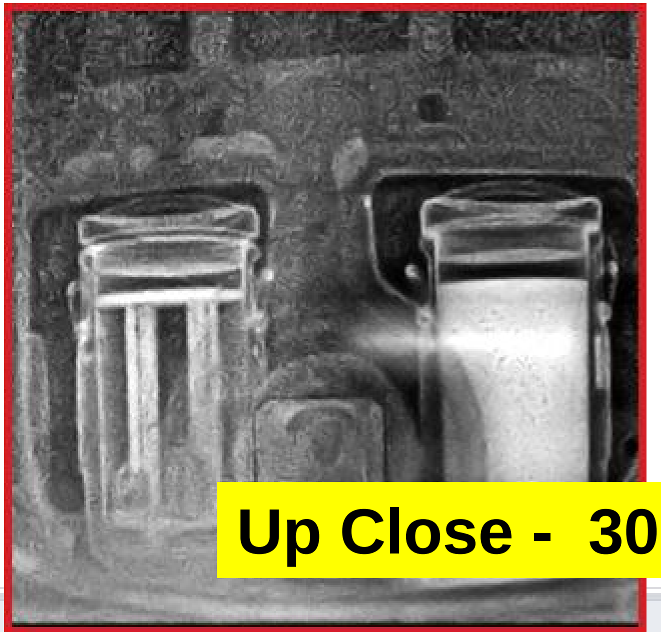
Robot-borne Miniaturized Backscatter Imager in Action

User gets two useful capabilities



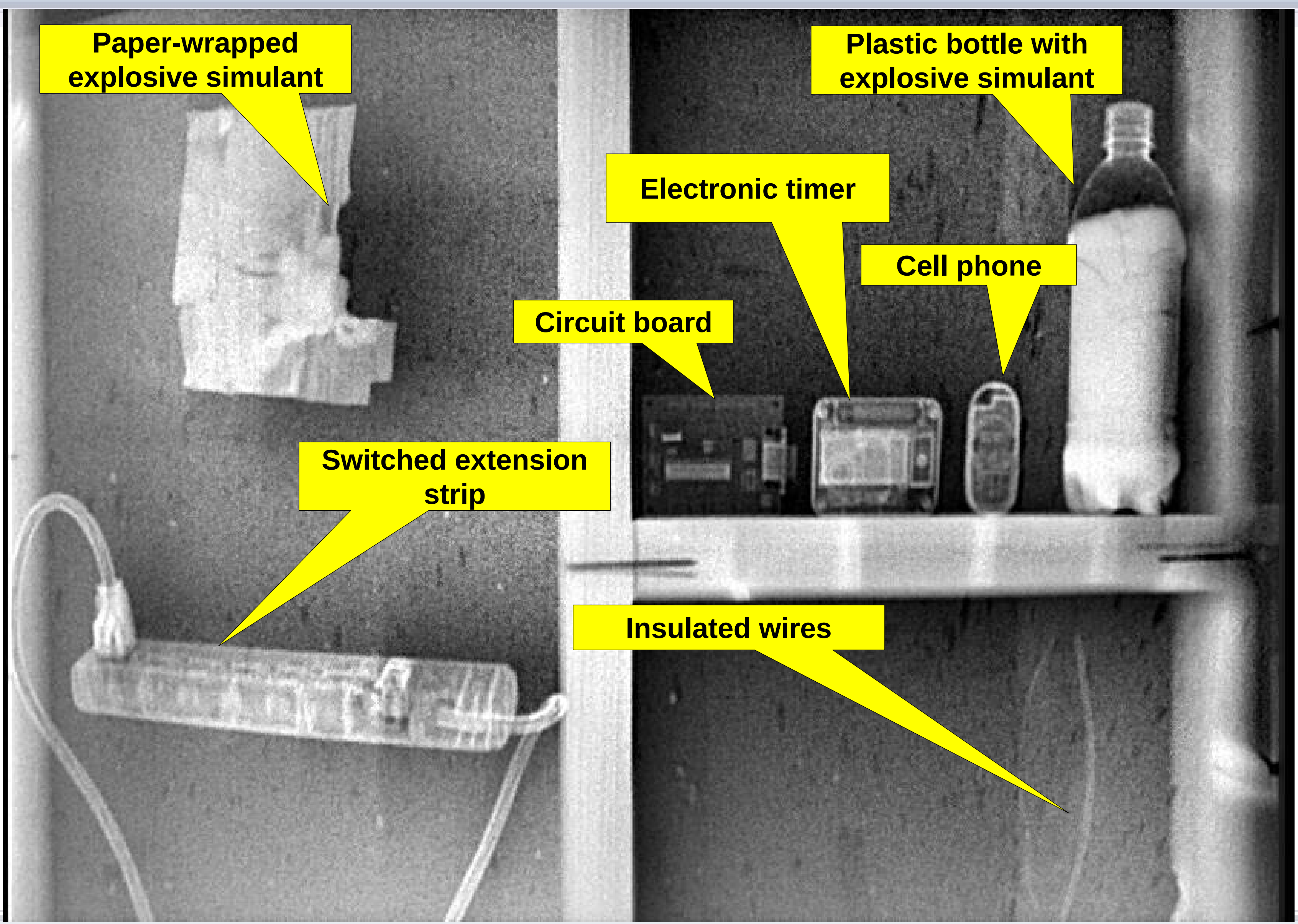


Standoff from 10 feet



Up Close - 30 in.

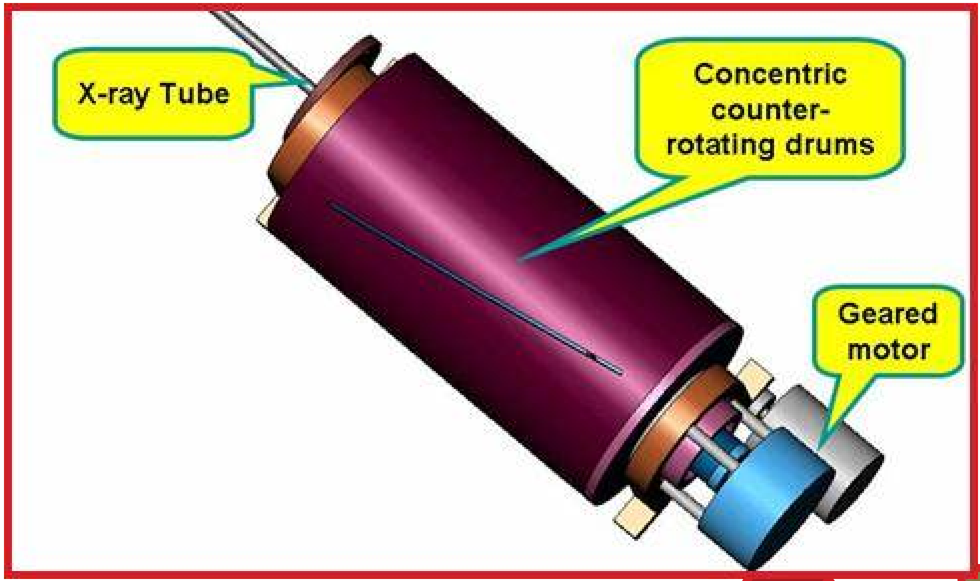
Image Into a Wall

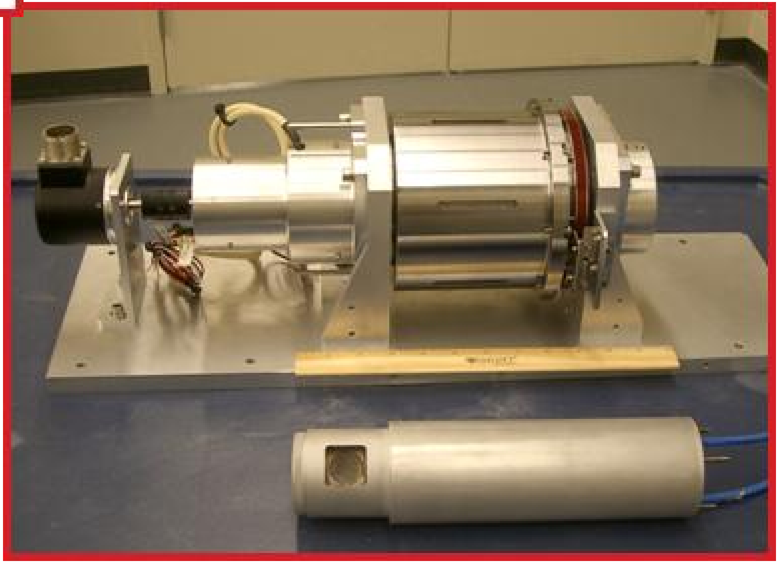


Dual Drum Imaging Concept

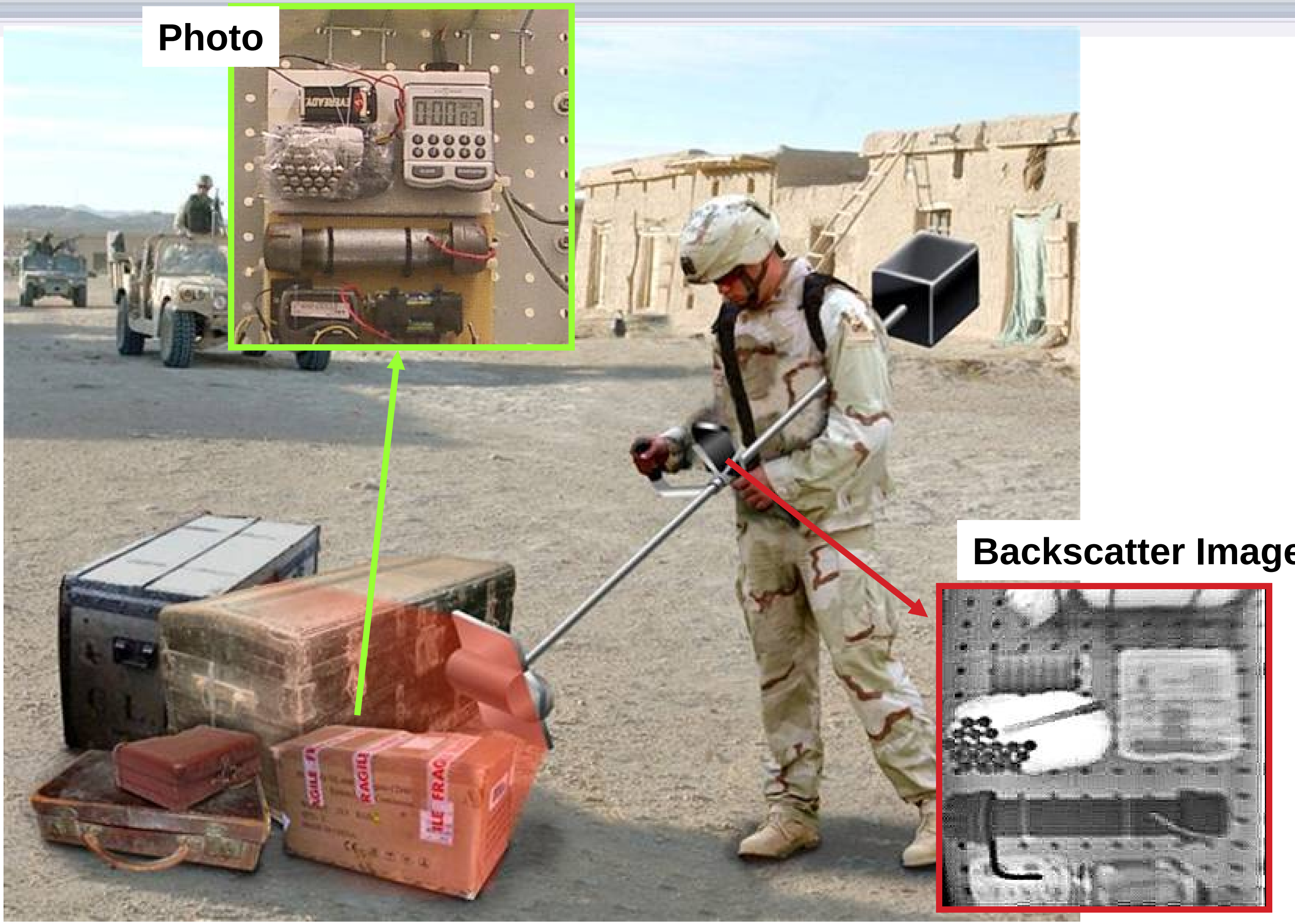
- Army/RDECOM/I2WD funded project
- No “external” motion required
  – Counter-rotating scanner drums create two dimensional image
- Imaging area and resolution determined by system size and distance from object scanned
- Image gets better the longer you scan
  – Improved photon statistics
  – Allows for fast scans as well as more detailed interrogations
- Mounting/Transport scheme adaptable
  – Tripod mount
  – Robot/platform mount
  – Potential for man-portable system
- Trade-off analyses in progress

AS&E Dual Drum Scanning Technique

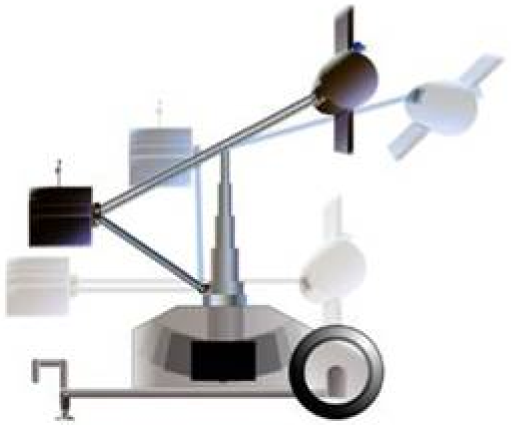




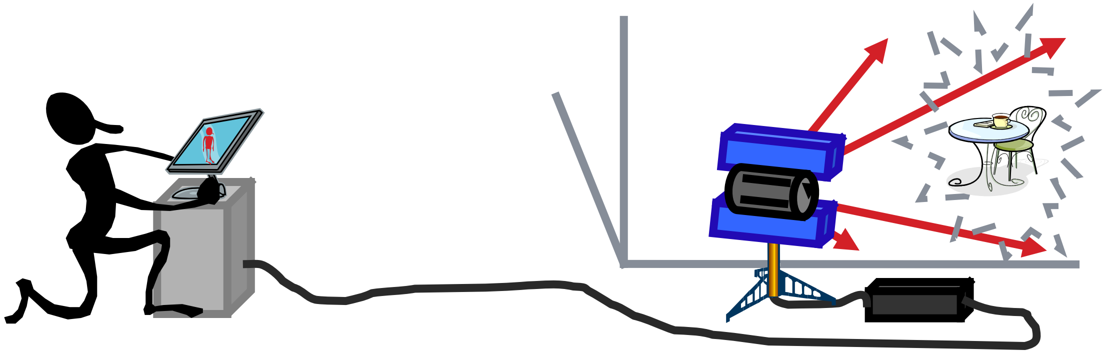
One Potential Application



Alternative Mounts and Applications



Trailer-mount

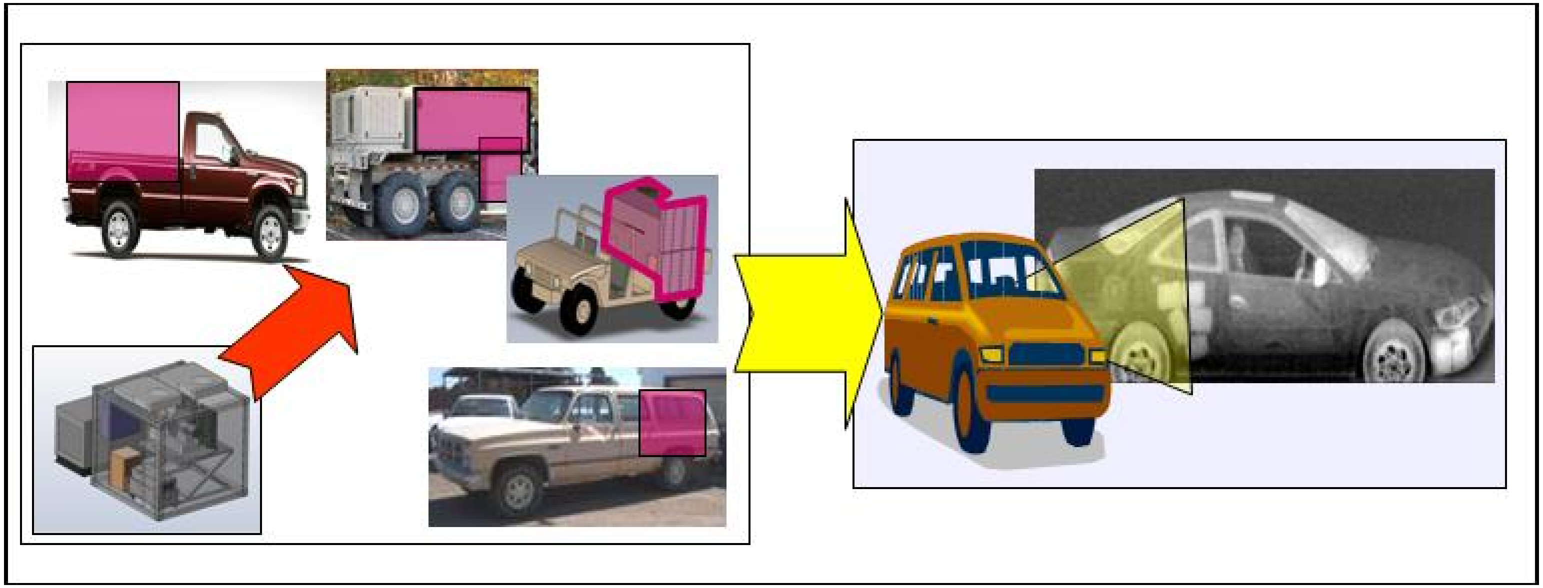


Thru-Wall Imaging

Robot-mount

Modular Backscatter

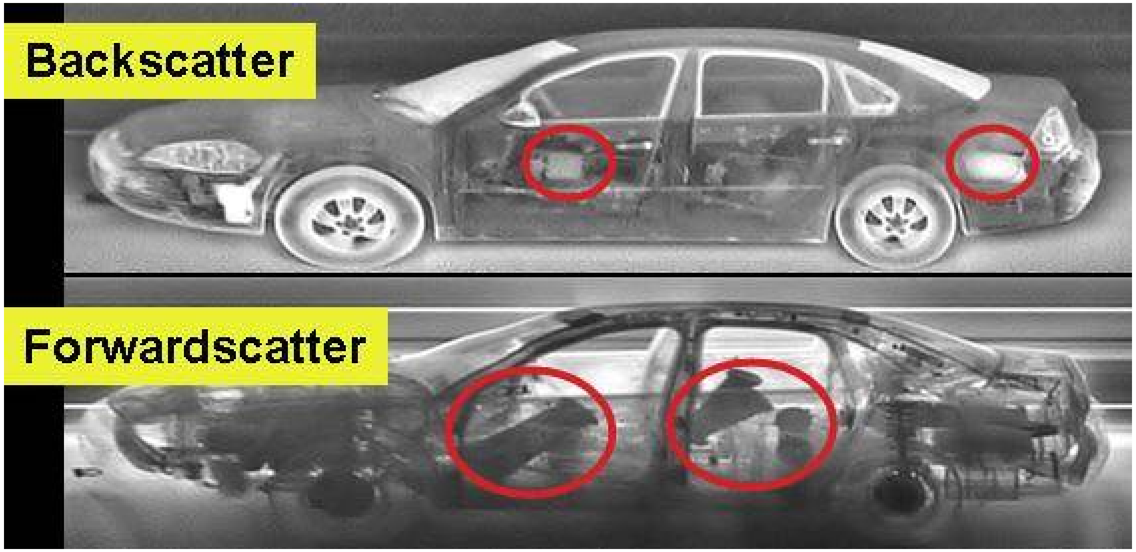
- Program sponsored by DHS S&T
- Explores system requirements trades and configuration/mounting alternatives to increase application base
- Selects and prototypes a modular system for evaluation



Trades and Requirements Definition in Progress

Supplemental Detectors Permit Additional Capabilities

- Better/Quicker Backscatter images
  - Increased scatter capture area improves S/N
- Potential for "stereoscopic" images
  - Allows offset detectors and independent channel processing
- Permits "Forwardscatter" imaging
  - Improved detection of high density materials in clutter



Where To Go From Here

- Operator Assist
  - Image processing/manipulation
  - Filters
  - Historical Comparison
  - Threat Identification
- Interface with others
  - Data sharing
  - Networking

More Information?

Bill Baukus, Director, Technology Development

American Science and Engineering, Inc.

Phone: (978) 262-8663

E-Mail: wbaukus@as-e.com

Website: www.as-e.com

The Real Estate Side of SCIF Space

Presented by Warren Amason

3 Things

- Process
- Deal Structure
- Lease Issues (legal landmines)

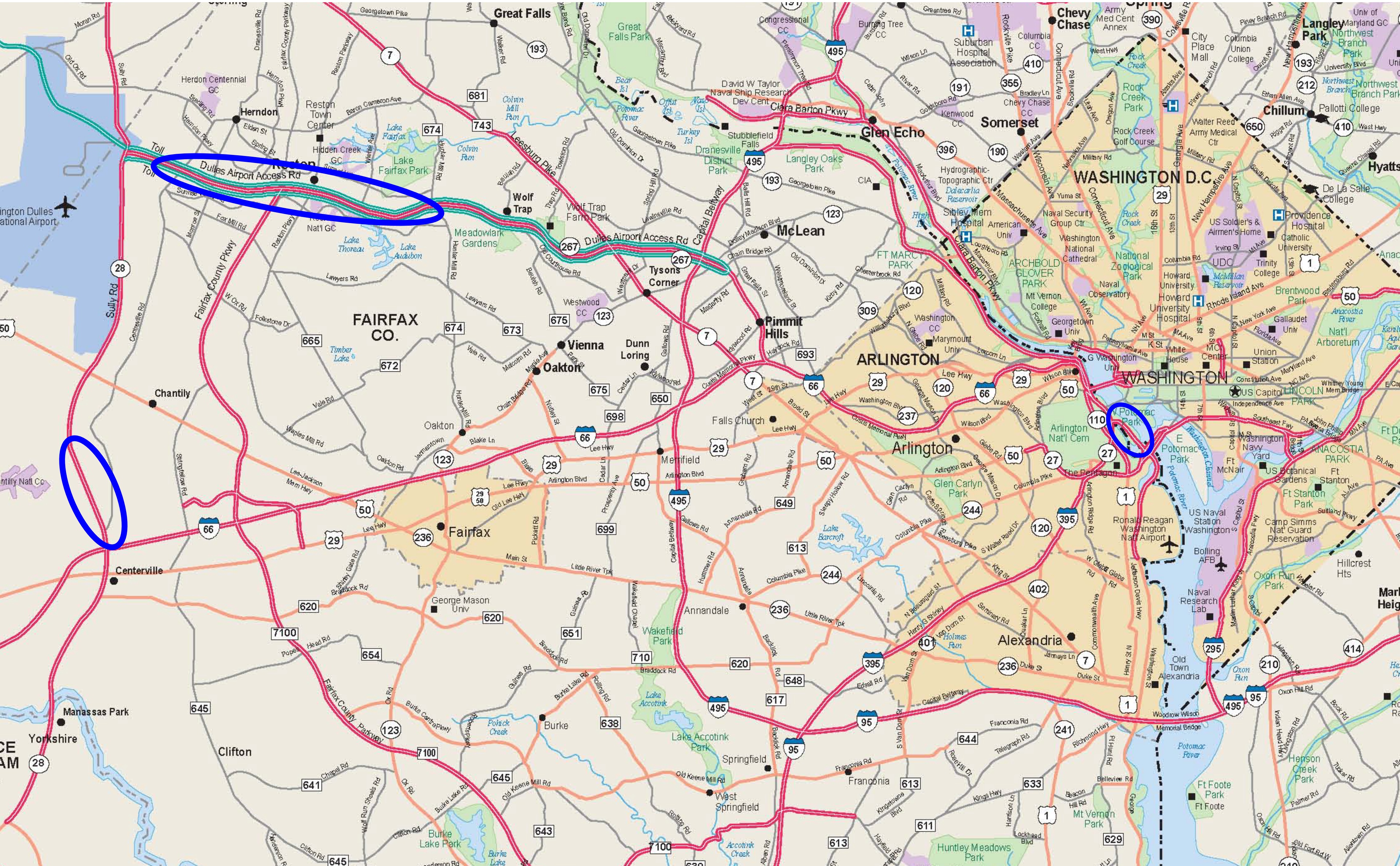
Process

GRUBB & ELLIS
From Insight to Results

- Timing
  - Shell space (new)
  - Existing

Map

GRUBB & ELLIS
From Insight to Results



Deal Structure

- Landlord contribution to cost
  - Term
  - Amortize into rent

Lease Issues (legal landmines)

- Lease commencement
- Access
- Proximity Issues
- Restoration
- Holdover

Lawrence Livermore National Laboratory

The Business Case for a Public-Private Sector Partnership in High Performance Computing (HPC)

Roger W. Werne, Ph.D.
Deputy Director, Industrial Partnerships
October 15, 2009

Lawrence Livermore National Laboratory, P. O. Box 808, Livermore, CA 94551

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344

LLNL-PRES-41224

The Business Case for a Public-Private Sector Partnership in High Performance Computing (HPC)

My talk will focus on three questions:

1. Why is HPC really important to business and government?
2. What are some "market" examples in business and government?
3. What kind of partnership makes sense?

Richard W. Hamming – circa 1957

"The purpose of computing is insight not numbers"

"Machines should work. People should think."

And insight is about creativity, options and ultimately decision making

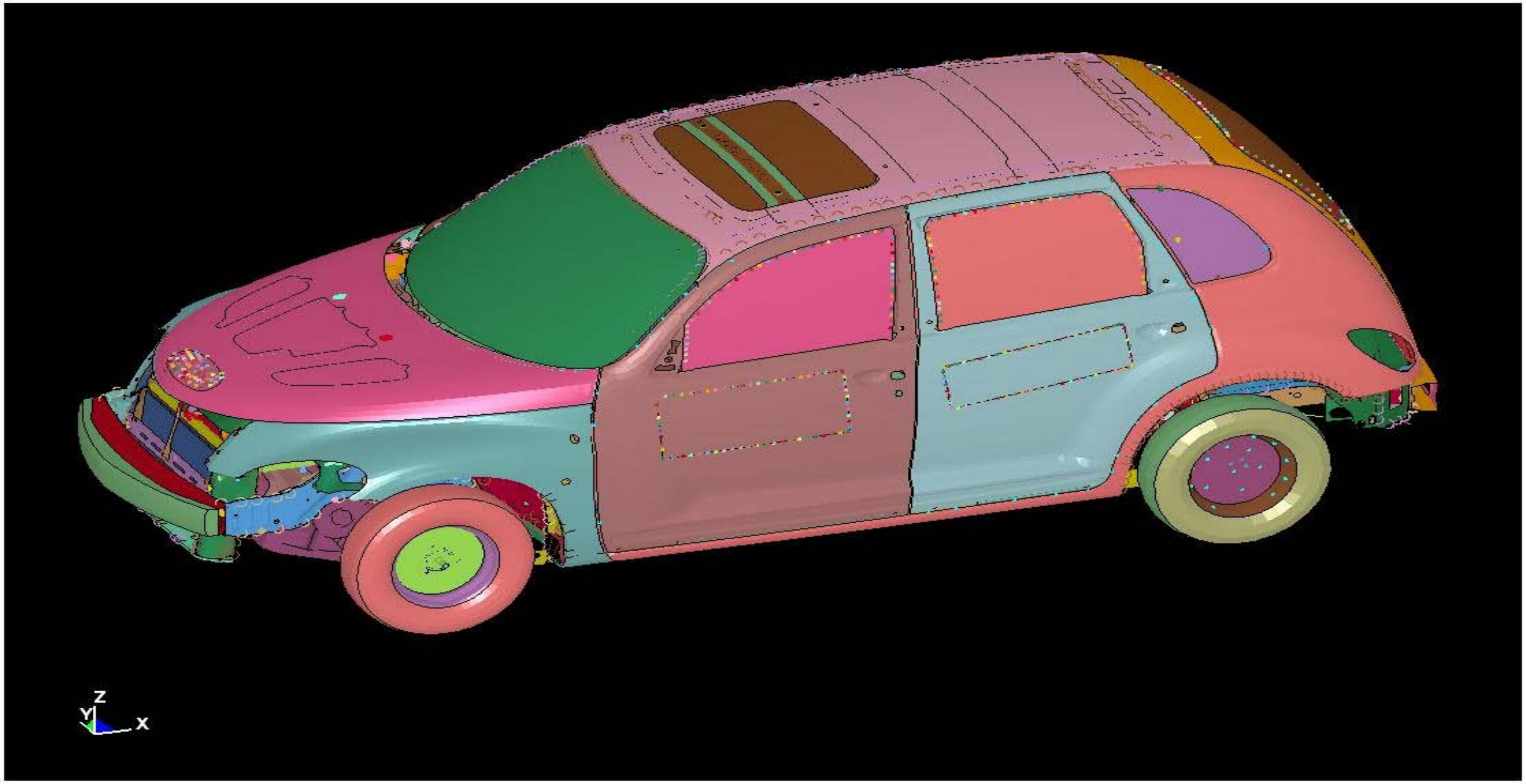
- Creativity is inventiveness, originality, thinking of things in new and different ways – exploring the unknown through numerical experiments, data mining, etc.
- Options are choices, pathways forward, alternatives – analyzing more design options within a given period of time
- Decisions are options, choices, pathways, or alternatives selected as a path forward – decisions that make your business “better, faster, cheaper”

Many industries/sectors have recognized the value of computing and are investing significant resources in predictive simulation

- Automobile and aircraft – performance optimization
- Oil and gas – seismic mapping, resource recovery
- Infrastructure management – emergency response
- Pharmaceutical – drug discovery
- Finance – financial market analysis and “prediction”
- Environment – weather prediction, environmental prediction, global climate change

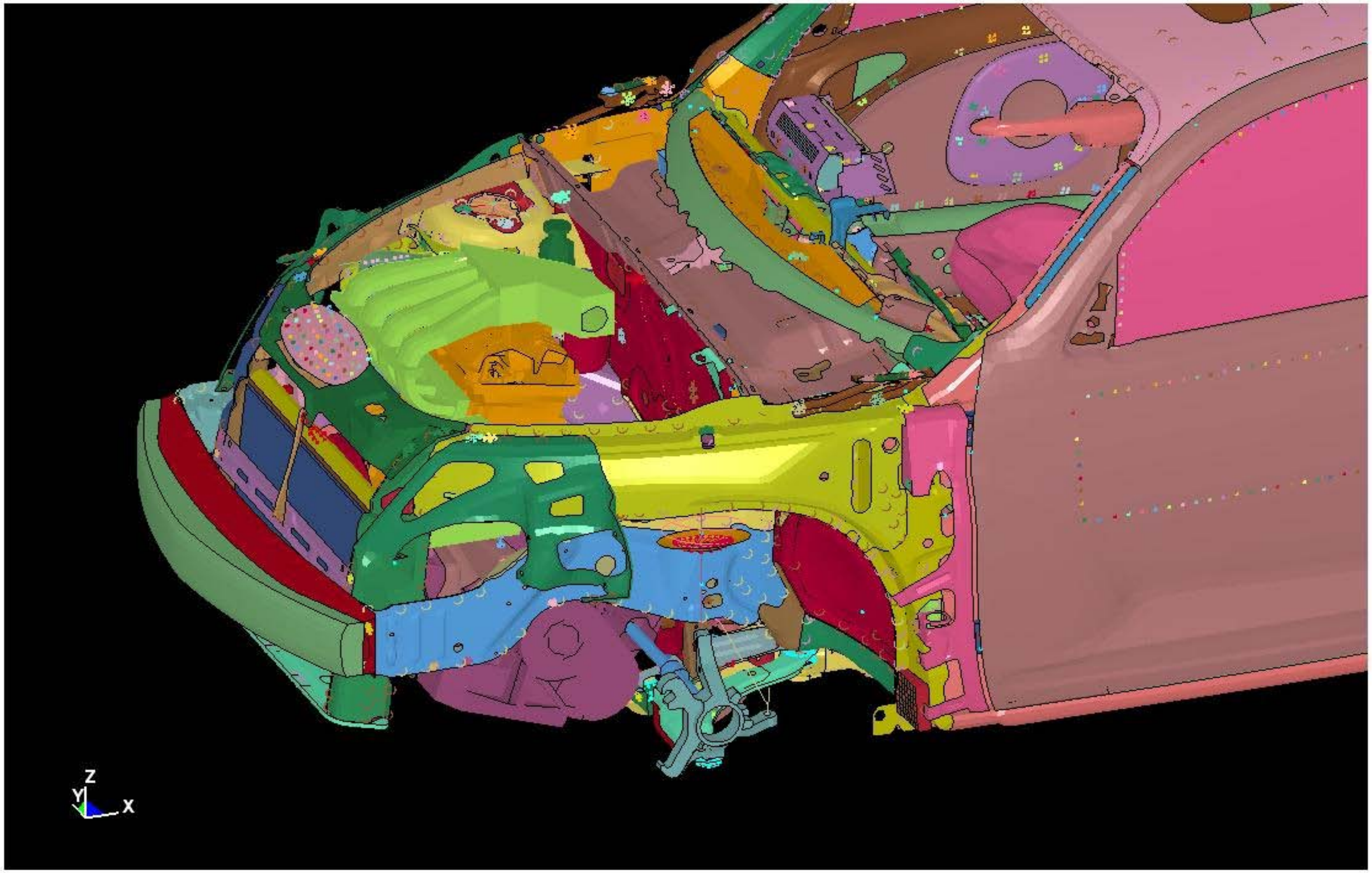
A few examples ----

Automotive Market: In the late '80s the DYNA3D code, commercialized as LSDYNA by Livermore Software Technology Corporation, revolutionized crash simulation in automotive design*

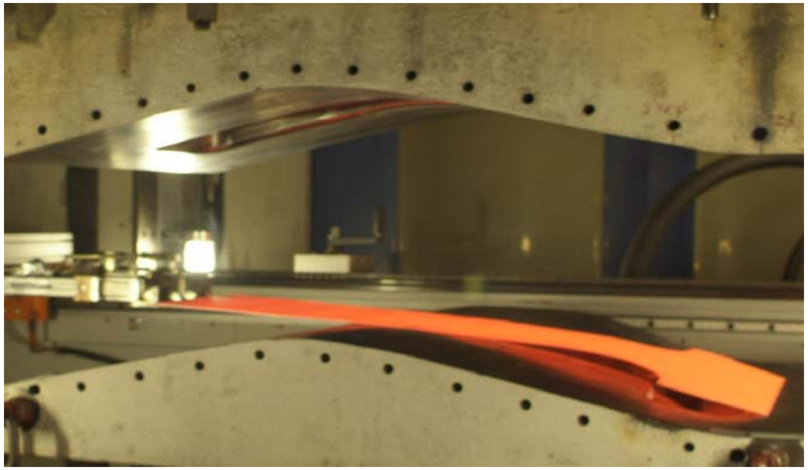


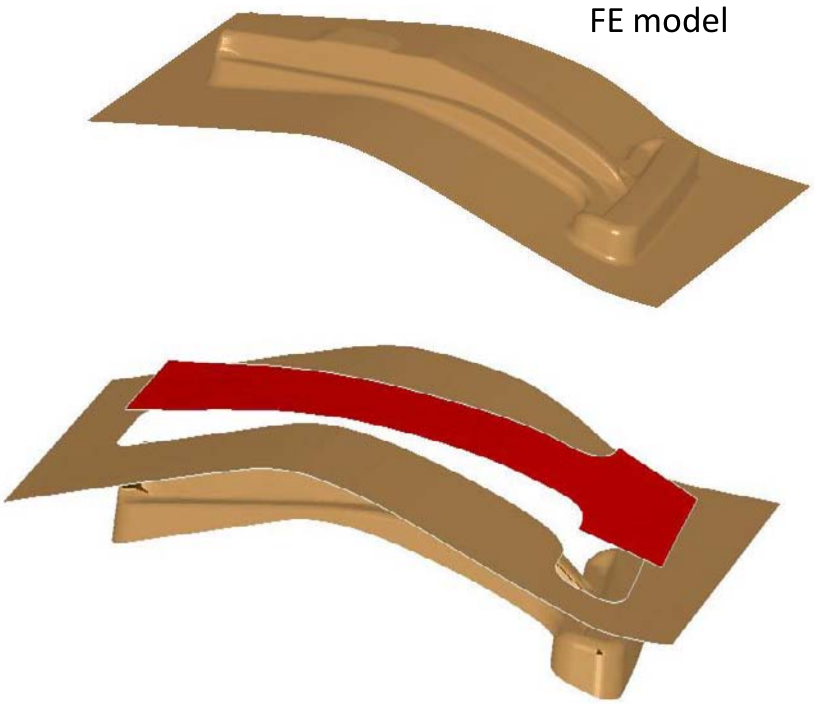
*compilments of Art Shapiro, PhD, LSTC

Detailed structural models, which include body structure, and spot welds, suspension, and tires allow crash safety to be analyzed without expensive full scale testing



Manufacturing: Thermo-mechanical Models of the manufacturing process also save time and money - a goal is to model the manufacturing of the part and insert it, residual stresses and all, into the assembled automobile model*

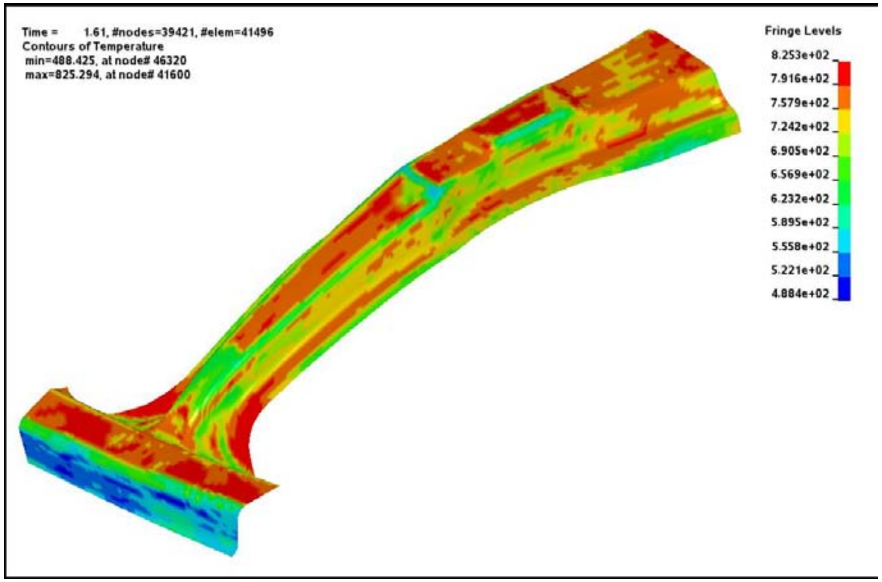




* Compliments of Art Shapiro, PhD, LSTC

Successfully "hot forming" a part requires accurate estimates of cooling rates which affect grain size and therefore material properties – therefore "time" is an important element in the manufacturing process

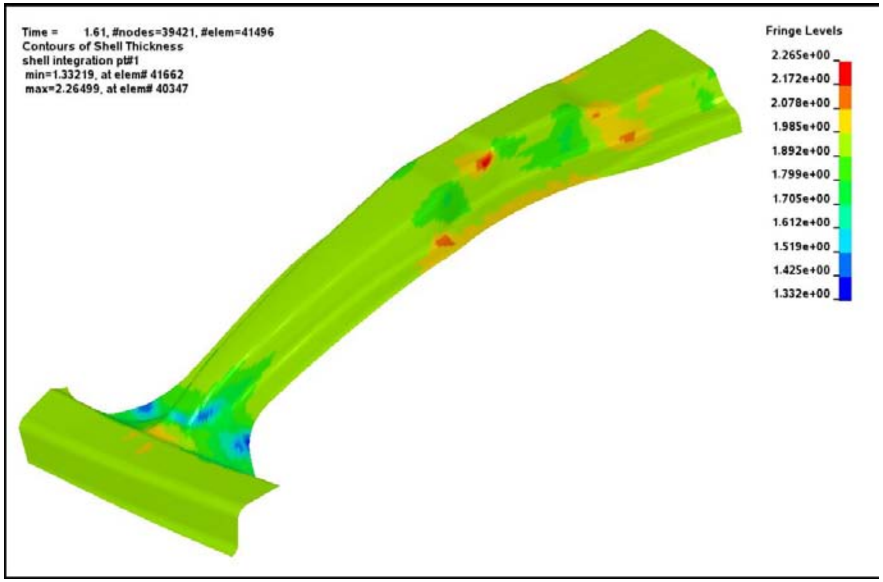
Results after forming



Temperature

min = 488C

max = 825C



Thickness

min = 1.33mm

max = 2.26mm

Studies show that scaling a given code to many processors is not straight forward*

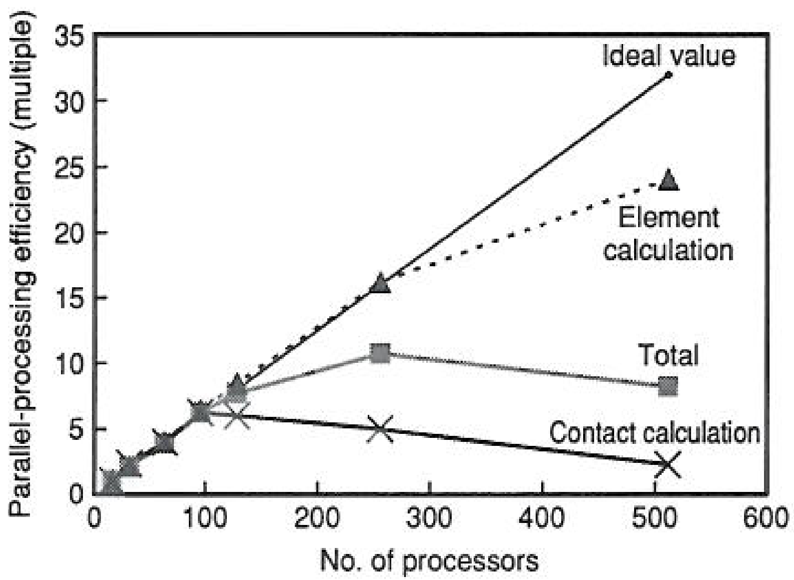


Figure 1
Parallel-processing efficiency for a 10-million-element model (before performance improvements).

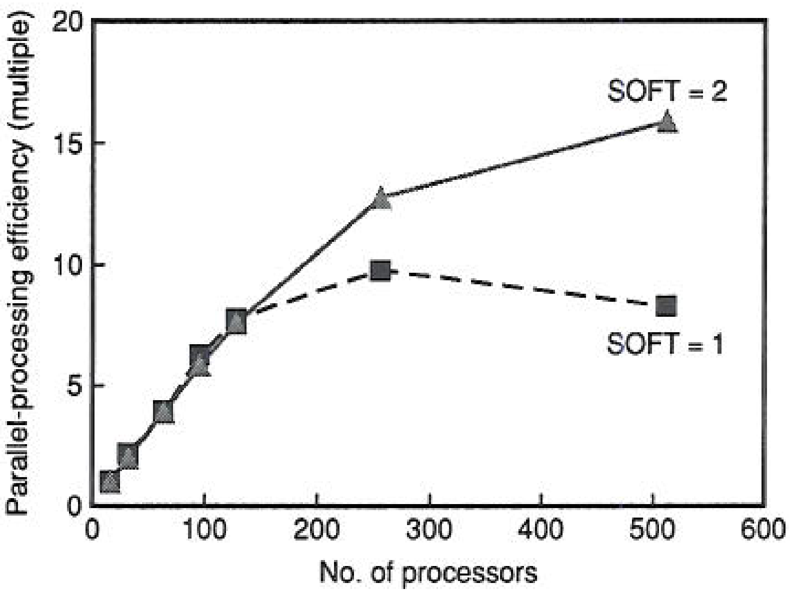
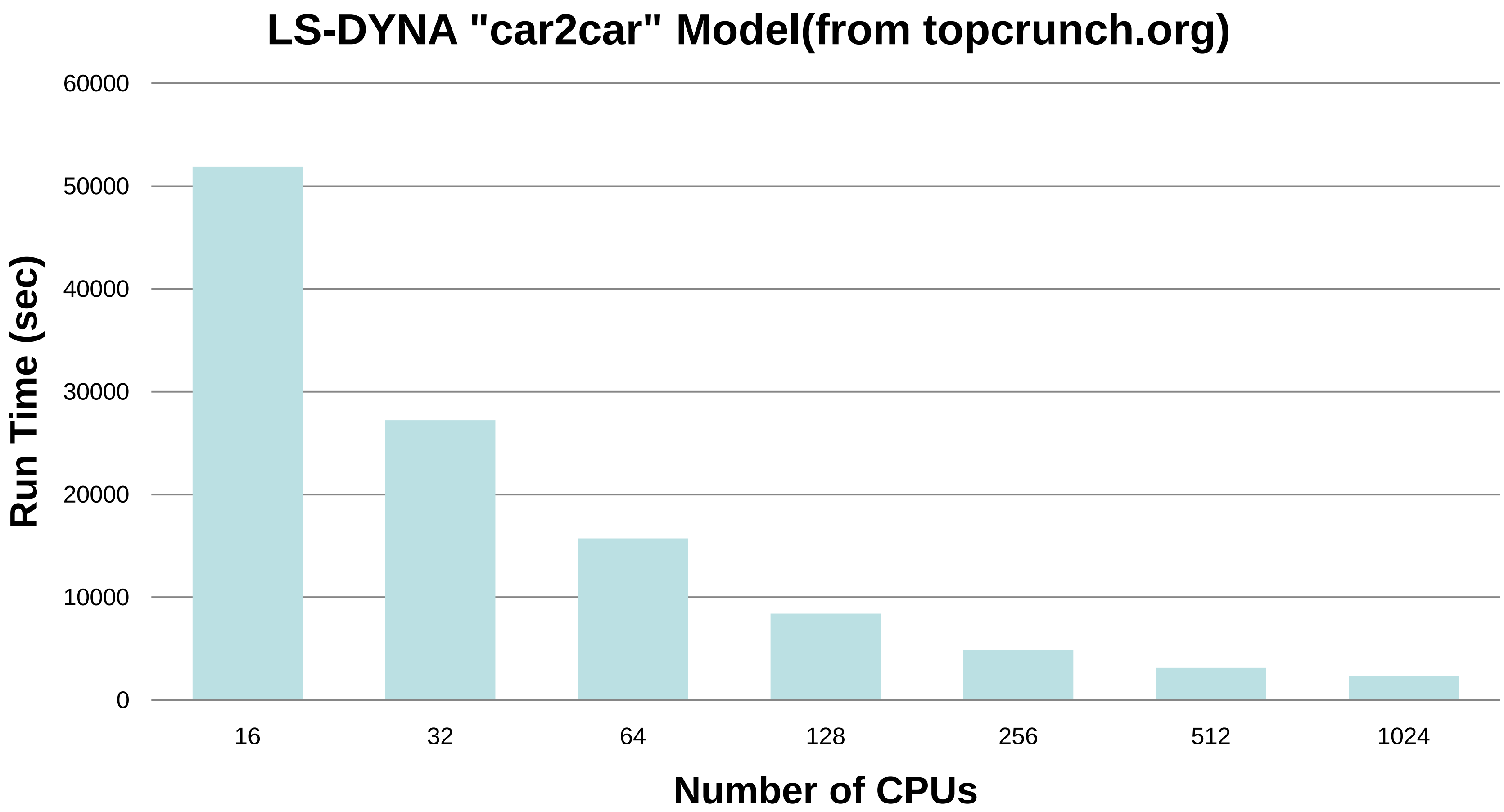


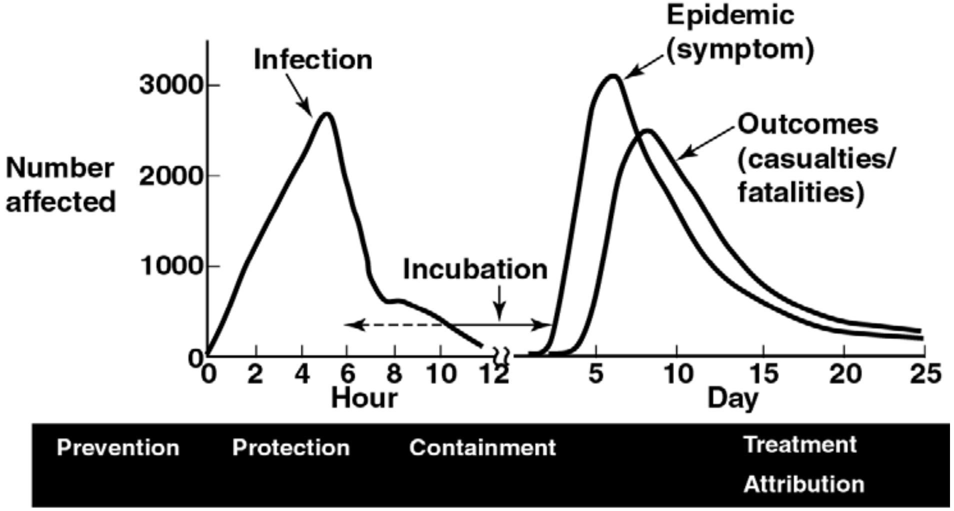
Figure 2
Parallel-processing efficiency for two types of contact definitions.

* Kondo & Makino, FUJITSU Sci.Tech. J. Oct. 2008

LS-DYNA scales very well with the number of processors



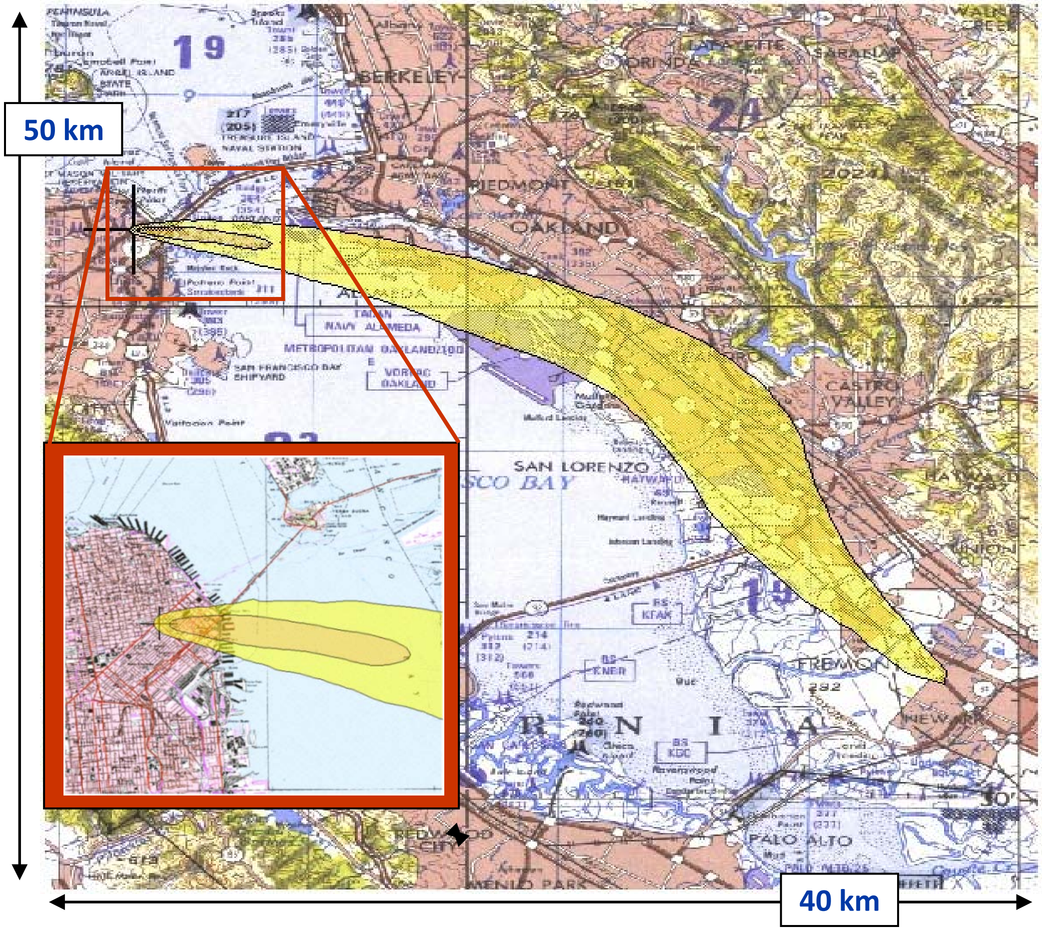
Homeland Security: Biological weapons represent significant threat because they are difficult to detect until symptoms appear



- Infections can usually be cured if vaccinations are given before symptoms manifest (within days)
- Detect to treat is the strategy ----

The threat is real --Aum Shinrikyo Headquarters — 1993

What appears to be a local WMD event can quickly become a regional problem*



Hypothetical release at the Embarcadero in San Francisco

Bio-agent Dose

Color	Area (km^2)	Description
(orange)	3.3	15% of the exposed population could receive a lethal dose Population: 1600
(yellow)	148	2% of the exposed population could receive a lethal dose Population: 308,192

Release location:

In the San Francisco Financial District

At 3rd and Market Streets

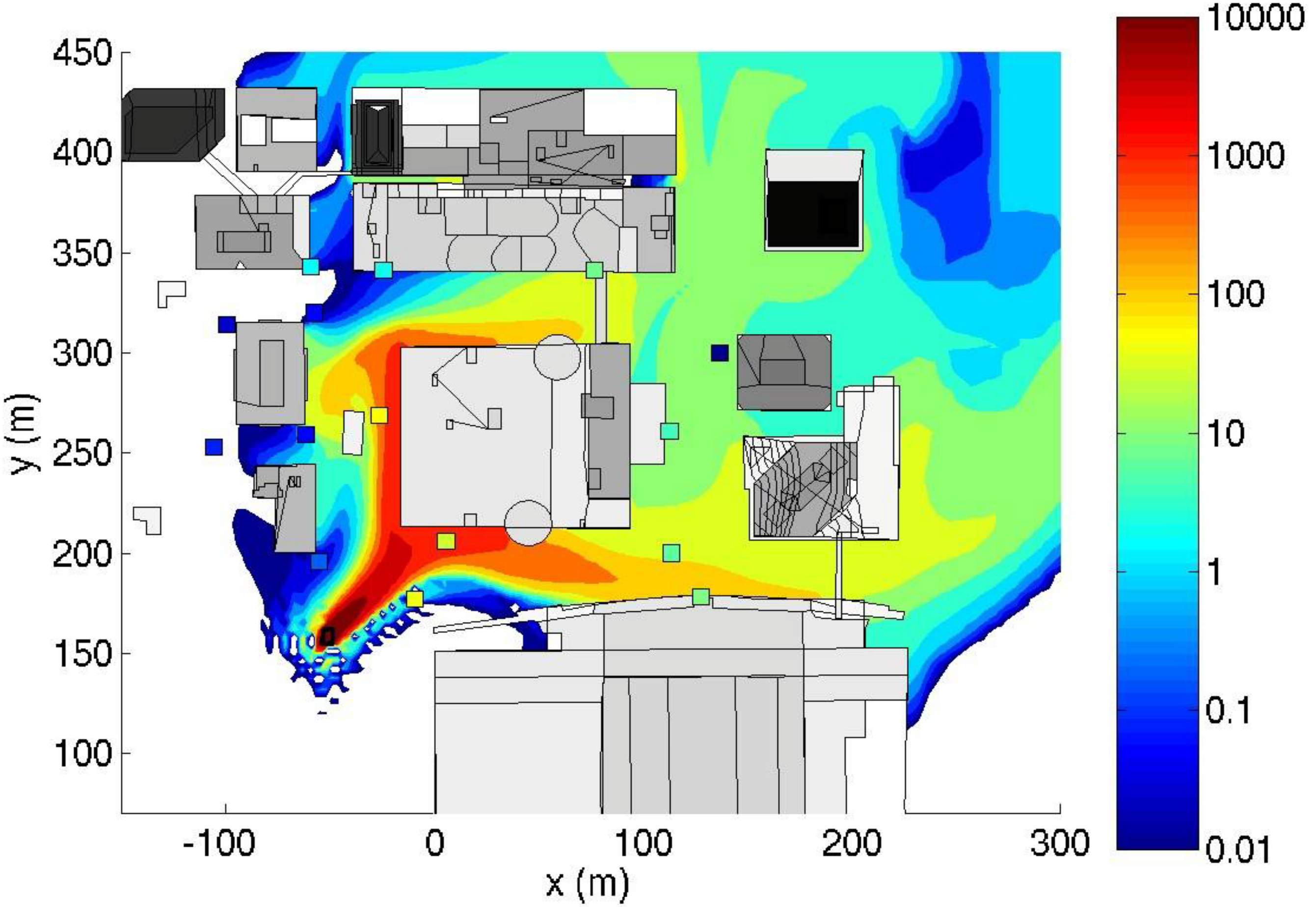
Lat/Long: 37° 47’ 14” N

122° 24’ 07” W

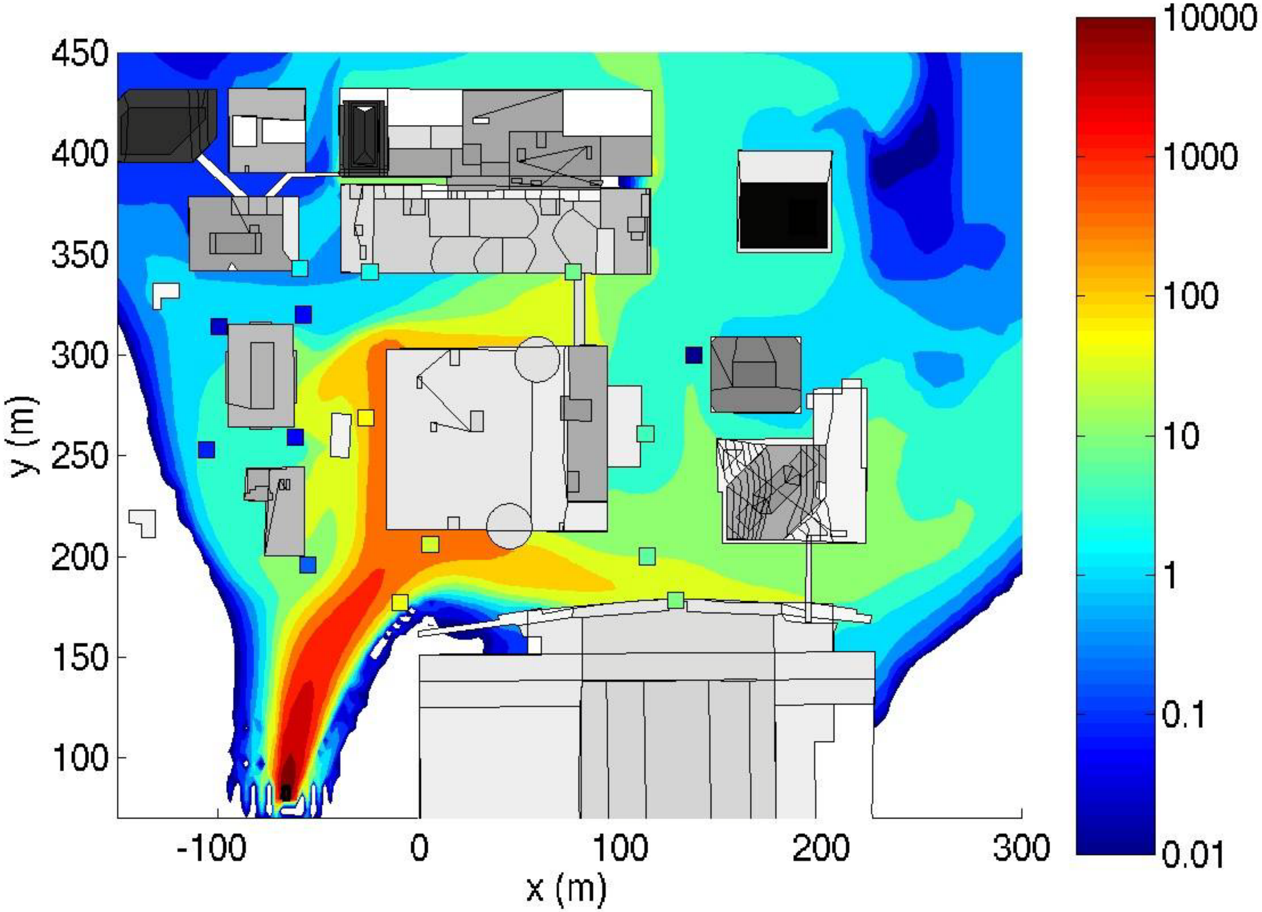
Meteorology: Observed winds at 5 PM PDT, 28 May 2003

*National Atmospheric Release and Advisory Capability

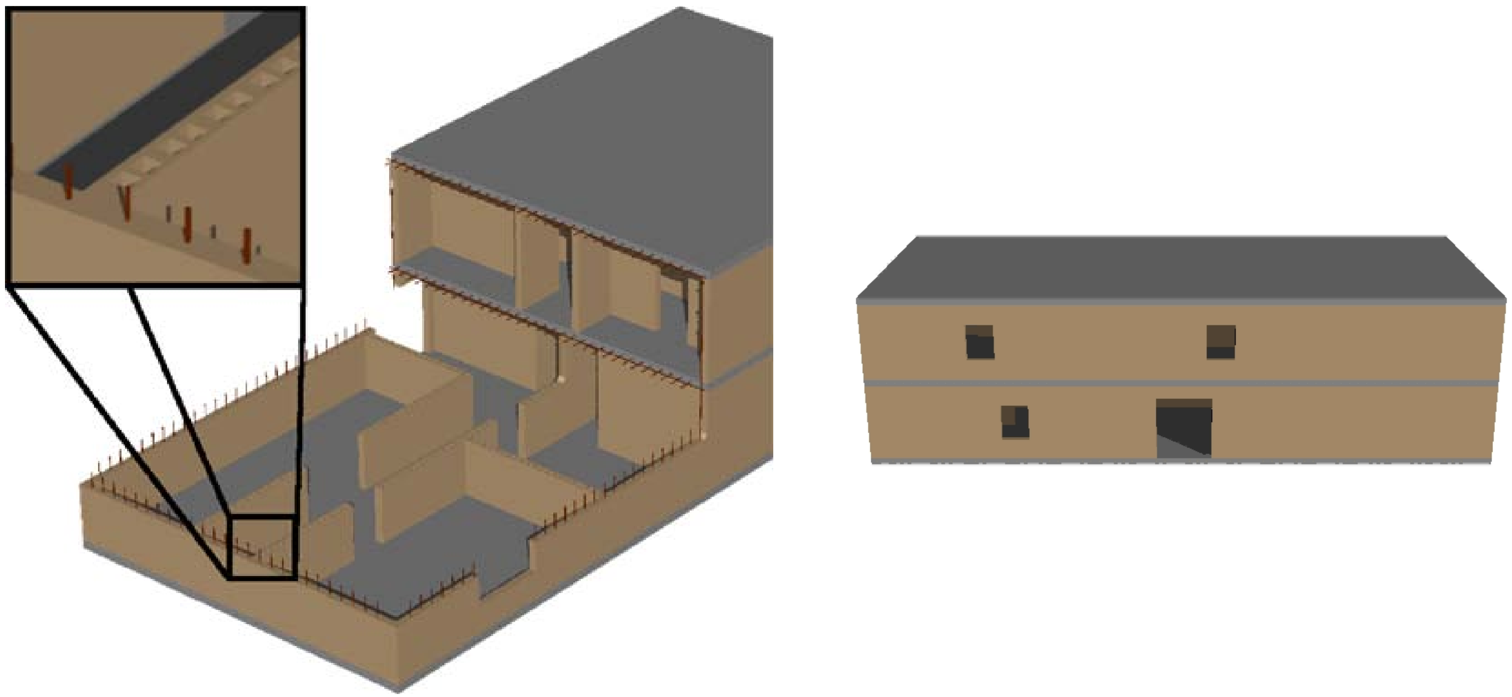
Locally, predicting source location in a complex flow environment is key – calculated flow from known source



Given “field measurements”, predict the source location, i.e., solve the inversion problem – much more difficult!



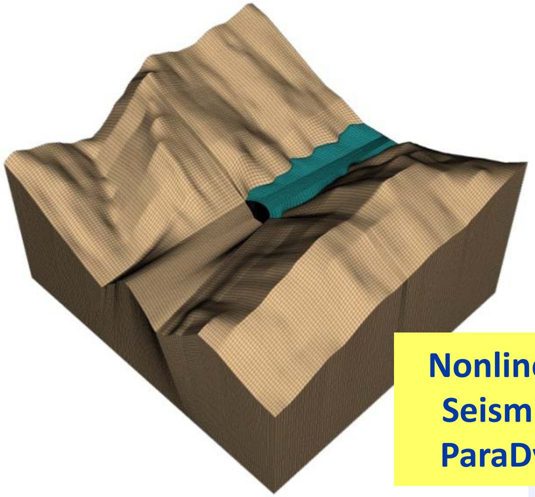
Infrastructure: A 10B zone 3D EM problem was calculated to study radar reflections from the interior surfaces of buildings.*



*compliments of Mark Stowell, PhD, LLNL

Infrastructure Management: Nonlinear seismic analysis of concrete dams*

- "In the design of practically all dams the difficulties of analysis are so great the consequences of failure so serious, and the cost of appreciably changing the probabilities of failure are of such high magnitude that refined model and analytical studies are almost always in order." – Newmark & Rosenblueth

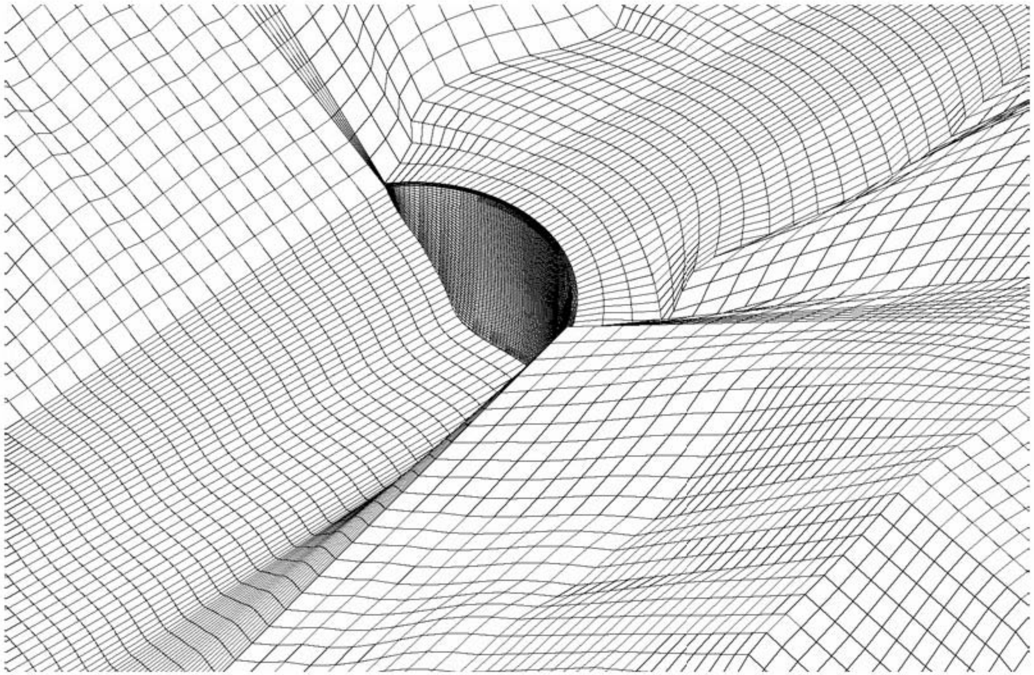


Nonlinear Seismic: ParaDyn

So, if one wishes to assess, through computational simulation, the integrity of a large concrete arch dam under realistic seismic excitation, then what aspects of this enormously complex problem must one truly get right?

*compliments of Chad Noble, PhD, LLNL

3D dam/reservoir/foundation finite element model of Morrow Point Dam



ParaDyn Model

1,071,625 solid hexahedral elements

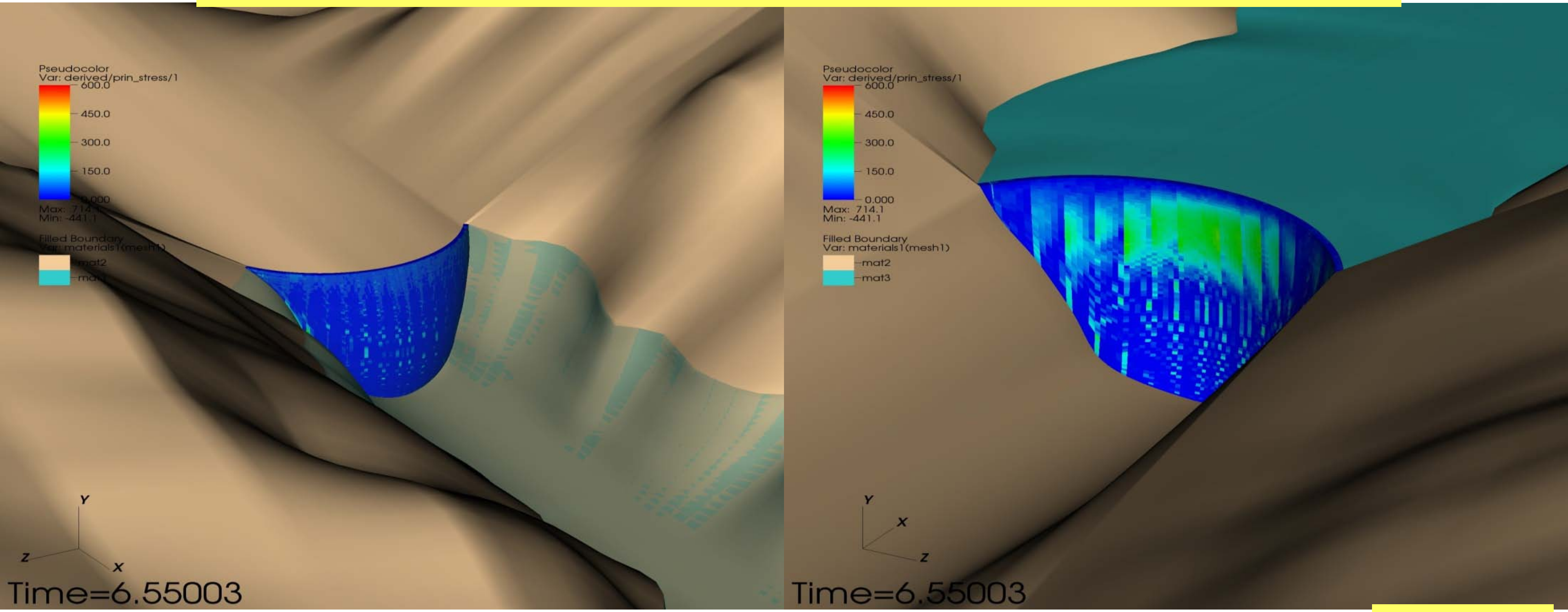
1,120,280 nodes

32 processors on MCR (LLNL)

Principal tensile stress at maximum displacement

Maximum displacement at T = 6.55 seconds predicted to be

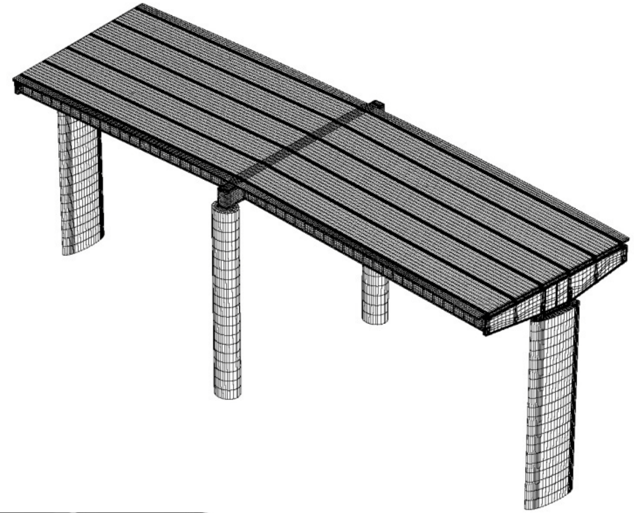
2.4 inches in the upstream direction



No significant damage predicted from M6.7 earthquake

Nonlinear Seismic: ParaDyn

Highway 580 Bridge Collapse due to a truck fire on *April 29, 2007 at 4:02 AM**



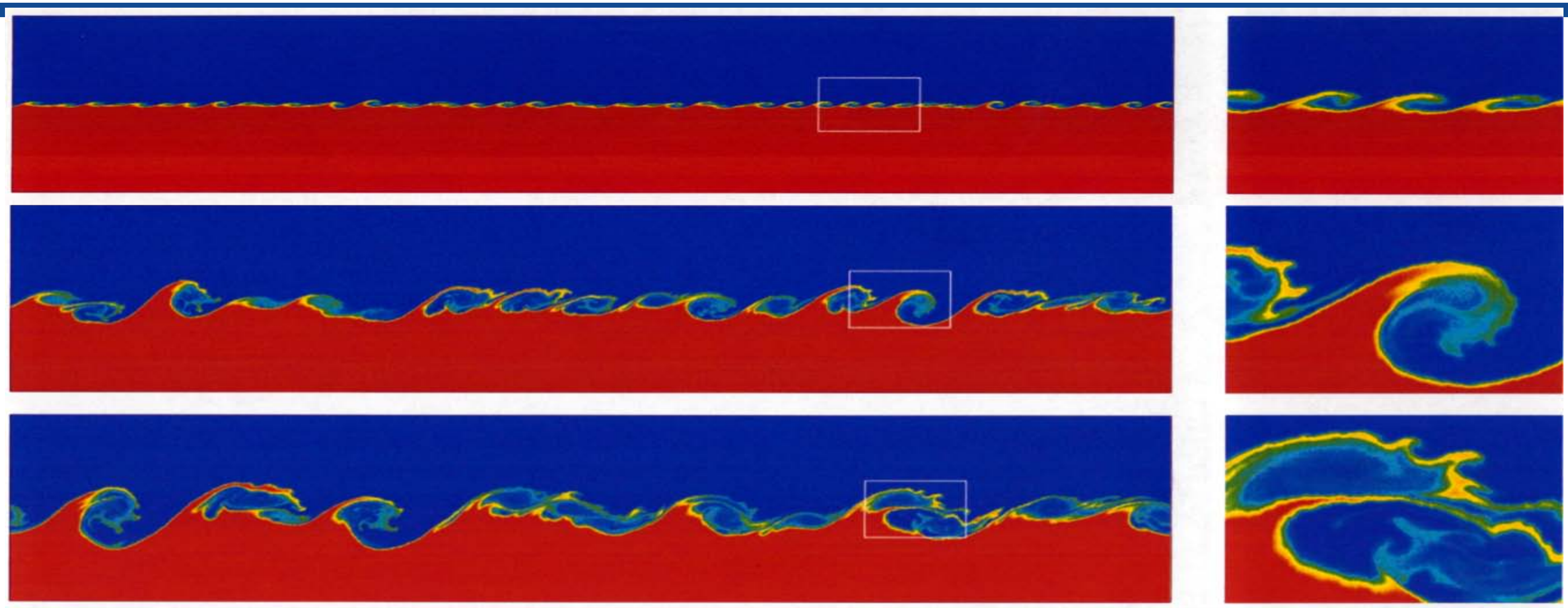
Objective: validate computer simulation so that effective fire and progressive collapse mitigation measures can be studied

Nonlinear thermal/structural:

TOPAZ3D/NIKE3D/DIABLO

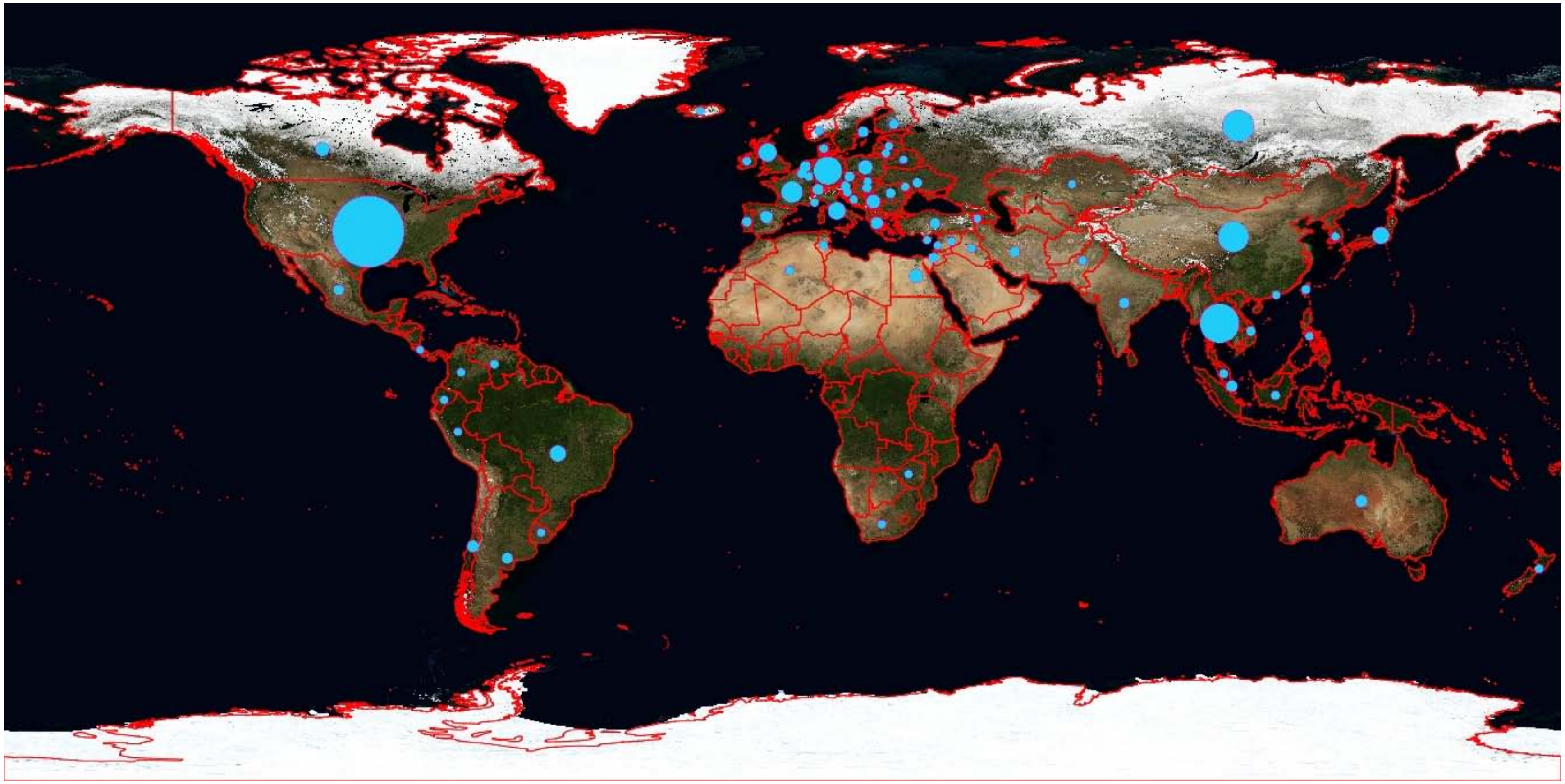
* compliments of Chad Noble, PhD. LLNL

Research: Computational Experiments - Initiation of Kelvin-Helmholtz Instability using Molecular Dynamics Simulation



- **Molten metals of differing densities undergoing a constant shear**
- **5.0 µm x 2.9 µm simulation of more than 2 billion atoms using ddcMD code for 8 days on all 131,072 processors of BGL - finalist for 2007 Gordon Bell Prize**
- **First atomistic simulation to develop Kelvin-Helmholtz instability at hydro scale**
- **This is the moral equivalent of Ab Initio 2D Hydro**

The HPC market is predicted to be > $15.5B in 2011. An example of interest: VISTA an LLNL open source HPC code: Over 88,000 downloads worldwide in 2007



The businesses in the HPC market fall into three categories

1. The **Users** who utilize HPC to better compete in their markets

2. The **Independent Software Vendors (ISVs)** who develop and sell the HPC tools to the **Users.**

3. The **Computer Vendors (CVs)** who sell hardware and operating systems to the **Users** and **ISVs**

The "Users" are the ones with the business problems to solve; they drive development of the ISV's and CVs

- In terms of "Decision Making", time is always of the essence for the "Users". For example:
  - Financial markets – seconds to months
  - Oil and gas – days to months
  - Auto and Aircraft – hours to days
  - Emergency response – minutes to hours
  - Infrastructure management – days to months

Increasingly, the Users are requiring larger predictive simulation problems to be solved in shorter periods of time: better, faster, cheaper decisions

However, the barriers to entry for the Users are significant

- Cost of the tools – start-up costs for hardware, software and personnel training can be significant as can be maintenance costs.
- Cost of money – many businesses want a factor of ten in five years, i.e., 58.5% discount rate. Or at least three-year payback or 28% per year.
- Resistance to change – “We’ve always done it this way; there’s no need to change”.
- A new level of intellectual sophistication is required in the business

So how do we lower the barrier for businesses wanting to become more competitive through the use of HPC resources?

- At LLNL, we believe that one answer is a Public-Private Partnership between a National Laboratory and businesses in the HPC market, e.g.,

Hyperion

A state-of-the-art HPC facility located at
Lawrence Livermore National Laboratory

Hyperion Collaborations Allow Partners to Build A Resource None Could Afford Alone

Founding Members:

- **Intel, Dell, and Supermicro**
  - Processors, Nodes, Racks and Integration
- **QLogic, Cisco and Mellanox**
  - IBA switches & HCAs
  - Ethernet switches & NICs
  - IBA□Ethernet routers
- **DDN, Sun, LSI**
  - Storage Hardware
- **RedHat**
  - Linux Testing and System Admin
- **Sun and RedHat**
  - Parallel File Systems

28

Hyperion* is next generation Linux cluster and is the largest testbed of its kind in the world

- 1152 nodes – 9216 cores
- 100-teraFLOP/s peak
- > 9TB memory
- InfiniBand 4X DDR interconnect & access to > 47 GB/s Raid disk bandwidth
- Two storage area networks(Data Center Ethernet & InfiniBand)

*for further information contact Mark Seager, PhD, LLNL.

The benefit to Hyperion commercial partners is competitive advantage

- Access to a world-class HPC capability at a reasonable cost
- Access to LLNL’s and partners’ expertise in HPC
- Shared risk with other parties
- Test new hardware and software products in a demanding HPC environment – try before you buy!
- Low risk approach to explore new capabilities/possibilities

Benefits to LLNL are also significant

- Access to the latest hardware and software
- Access to many smart people in industry
- Ability of LLNL to help U.S. industry maintain leadership in the competitive HPC world market
- Help LLNL understand HPC commercial market directions

Contact Information:

- Roger W. Werne, PhD
- Deputy Director – Industrial Partnerships
- Lawrence Livermore National Laboratory
- PO Box 808, L-795
- Livermore, CA 94550
- Phone: 925-423-7302
- Email: werne1@llnl.gov

Super Empowered Individuals

Man?

Myth?

Does it matter?

What are the implications?

William W. Coffey

NDIA Disruptive Technology Conference

October 13-14, 2009

The Telesti Group

Advice Focus Support

Overview

- Caveats
- What is it?
- What is the history?
- How will it affect us?
  - Society
  - Warfare
- How do we deal with?

Caveats

- Locate, Close with and Destroy the enemy
  - Find, Fix, Finish
- Machines don't fight wars. People do, and they use their Minds.- Col John R Boyd
- Principles of Warfare still apply
  - War is the extension of politics by other means- Clausewitz
  - If you know the enemy and know yourself you need not fear the results of a hundred battles – Sun Tzu
- Just because we want to believe it does not make it true- Unknown

Impact of Technology

- “People always overestimate what they can do in one year and *underestimate* what they can do in 10.”- William Gates Founder Microsoft
- “650k ought to be enough for anyone”- William Gates Founder Microsoft
- Overemphasis on the non-physical world is just as dangerous as ignoring it- William W. Coffey

What is it?

- **dis·rupt–**
  - 1. to cause disorder or turmoil in
  - 2. to destroy, usually temporarily, the normal continuance or unity of
  - 3. to break apart
- **tech·nol·o·gy**
  - 1. the branch of knowledge that deals with the creation and use of technical means and their interrelation with life, society, and the environment, drawing upon such subjects as industrial arts, engineering, applied science, and pure science.
  - 2. the terminology of an art, science, etc.; technical nomenclature.
  - 3. a technological process, invention, method, or the like.
  - 4. the sum of the ways in which social groups provide themselves with the material objects of their civilization.

- What is disruptive technology? The simple answer is a technology that disrupts.
- Disruptive in Context Only

Super Empowered Individuals (Dictionary.com)

- **Super -**
  - a prefix occurring originally in loanwords from Latin, with the basic meaning “above, beyond.” …More figuratively, “an individual, thing, or property that exceeds customary norms or levels” (superalloy; superconductivity; superman; superstar), “an individual or thing larger, more powerful, or with wider application than others of its kind” (supercomputer; superhighway; superpower; supertanker), “exceeding the norms or limits of a given class” (superhuman; superplastic),
- **em·pow·er –**
  - 1. to give power or authority to; authorize, esp. by legal or official means: I empowered my agent to make the deal for me. The local ordinance empowers the board of health to close unsanitary restaurants.
  - 2. to enable or permit: Wealth empowered him to live a comfortable life.
- **in·di·vid·u·al-**
  - 1. a single human being, as distinguished from a group.
  - 2. a person: a strange individual.
  - 3. a distinct, indivisible entity; a single thing, being, instance, or item.
  - 4. a group considered as a unit.

- Individuals that can “take on the world”

Humanity - Technology

Technology	Changes
• Wheel	Transportation
• Flint	Means of production
• Copper	Means of production
• Iron	Means of production
• Printing Press	Literacy, Knowledge
• Interchangeable parts	Means of production
• Internal Combustion Engine	Transportation
• Wireless Technology	Communication
• World wide web (not Internet)	Literacy, Knowledge

War- Technology and Counter

Technology

- Raiding Party
- Castle Walls
- Tanks
- Mass Formation
- Aircraft
- What we do now
- Who knows

Changes

- Walls
- Canon
- Panzer Faust
- Repeating Arms
- 3rd Dimensional fight
- Who knows
- Still figuring it out

Societal Changes

Socio-Political

- Family
- Tribe
- City State
- Nation State
- Trans-National State
- Non-National State
- Non-State Actors

Socio-Economic

- Agricultural
  - Guilds
  - Cottage Industries
  - Limited Distribution of food
- Industrial
  - Mass Production
- Post-Industrial

“Disruptive” Technologies

Technology

- Google Earth Images
- Social Networking
- Cloud Computing
- Virtual Reality
- Biometrics
- Mash up
- Miniaturization
- Etc.

Displacement

- Library, Cartographers, surveyor
- Free Association, Assembly of individuals, face to face coordination
- Mainframes
- Etc.

Impact on Society

General Impact

- Means of production
  - Decentralization
    - Less Authoritarian?
    - Privatization?
  - More Transient
  - Shrink
- Defense industrial base
  - Knowledge Revolutionary Idea
- DIME

Developing World

- Globalization
  - Sat TV
  - Wireless Comms
  - Movement
- Migration
  - Emigration
  - Immigration

Impact on Warfare

- **M**ass
- **O**bjective
- **O**ffensive
- **S**ecurity
- **E**conomy of Force
- **M**aneuver
- **U**nity of Command
- **S**urprise
- **S**implicity

- Enemy is now super empowered individuals
  - Operating on behalf of…….

How to deal with it?

- Judo
- Think
- Move
- Communicate
- Multi-level capability
- Enable action
- Encourage action

How will it affect us?

- Change Attitudes
- Change Capabilities
- Change in responsibilities
- DOTMLPF

Questions?

CONTACT INFO: WILLIAM W. COFFEY
TEL: 503.302.6543
EMAIL:
WILLIAM.W.COFFEY@TELESTIGROUP.COM

Challenges and Opportunities in the Changing Science & Technology Landscape

(Capability Gap Changing Surprises – Avoidance and Exploitation)

Dr. Don Wyma

Director for Scientific & Technical Intelligence Analysis

Office of the Under Secretary of Defense (Intelligence)

National Defense Industrial Association

6th Annual Disruptive Technologies Conference, 14-15 October 2009

Slides are UNCLASSIFIED

Briefing is SECRET

Agenda

- What to talk about?
- S&T through the Intelligence Community (IC) lens
- Defense S&T intelligence analysis
  - Guiding documents
  - Current organization
  - Future capabilities
- Partnering opportunities

What to talk about?

- Reoccurring observations from previous NDIA meetings
  - Pace, scale, and complexity of technology increasing
  - Negative trends in US S&T education and workforce
  - Impact of globalization on S&T center of gravity
    - Nongovernmental, commercial, privatization, etc.
  - Asymmetry and uncertainty in the future battlespace
  - "Current" processes remain unsatisfactory
    - R&D funding, tech integration, info sharing, warning, decision support, etc.
  - US technology dominance no longer assured

Recognition that these are enduring issues.
This is our reality! Now what?

Looking at S&T through the IC Lens

Under Secretary of Defense for Intelligence
HON. James R. Clapper Jr.

Principal Deputy
Mr. Thomas Ferguson

Chief of Staff

Deputy Under Secretary of Defense Joint & Coalition Warfighter Support

Deputy Under Secretary of Defense Technical Collection & Analysis

- **Analytic Concepts & Strategies**
- Collection Concepts & Strategies
- Special Capabilities

Deputy Under Secretary of Defense Portfolio Programs & Resources

Deputy Under Secretary of Defense HUMINT, Counterintelligence & Security

Relevant USD(I) Roles & Mission

- Exercises planning, policy, and oversight over all DoD intelligence, CI, and security policy, plans and programs.
- Foster Defense intelligence planning, preparation, warning, and forecasting
- Serve as Battlespace Awareness Capability Portfolio Manager

As of August 17, 2009

S&T through the IC Lens – Pace, Scale, and Complexity

- Important advances/applications require multi-disciplinary approach
  - Unlike academia & industry, IC organization not conducive
- Increasing amount of S&T information openly available
  - Access issues improving, knowledge management situation worsening
- Next-gen sensors/systems – data hungry, on-board data fusion
  - Unprecedented demands for all-source intelligence, required for system functionality
  - Modeling & Simulation (M&S) increasingly necessary

S&T Education and Workforce Trends

- Relative decline in US science & engineering advanced degrees
  - Greater competition for technically-trained people
- Increase in foreign scientists trained in US and overseas
  - Knowledge transfer from US almost impossible to comprehend
  - Less visibility into underlying indigenous foreign S&T capacity
- Concurrent need for specialization and generalization
  - Stressors on the analytic core – from career path challenges to workforce currency to schizophrenia

S&T through the IC Lens –

Globalization and the S&T Center of Gravity

- Shift in S&T center of gravity over last half century from government to multi-national corporations (MNCs)
  - Intelligence oversight has not kept pace
  - Decentralized decision making & technology transfer greatly complicate collection

- Economic & social drivers increasingly influence tech development & integration into society
  - Traditionally hasn't been a focus of S&TI analyst

S&T through the IC Lens – Asymmetry and Uncertainty

- Impact of S&T across the range of potential engagements scenarios
  - Low-tech application to high-end potential
  - Balance resources & focus against near- and long-term threats

- Battlespace awareness encompasses all domains
  - Learning curve for cyber & human domains (non-kinetic)

- Compressed decision cycles with greater information expectations
  - Reuters versus Rand

S&T through the IC Lens – Unsatisfactory Processes

- Acquisition regulations modified over the last decade to emphasize flexibility, agility, & innovation
  - Role of intelligence has been diminished & pushed to the right

- Compressed decision cycles with greater information expectations
  - Traditional requirement-production process not adequate

US Tech Dominance No Longer Assured

- Foreign S&T efforts in certain topic areas may surpass US capability
  - IC must be able to both warn of threats & identify opportunities
  - Increase in quality and quantity of non-English language S&T

Partnering Opportunities

Pace, scale, & complexity

S&T education & workforce trends

Globalization of S&T capability

Asymmetry & uncertainty

Unsatisfactory processes

US tech dominance not assured

Expertise

&

Processes

S&T Intelligence Guiding Documents

2002 Defense Planning Guidance

Defense Warning Office: …establish by October 1, 2002 a defense warning office charged with identifying sources of increasing threats to US interests in critical regions. This office will also identify opportunities to affect adversary behavior prior to & in the early stages of a crisis.

Warning on Technology Development: ensure development of a robust foreign S&T assessment capability beginning in January 2003 to provide the earliest possible warning of technological developments that could undermine US military preeminence.

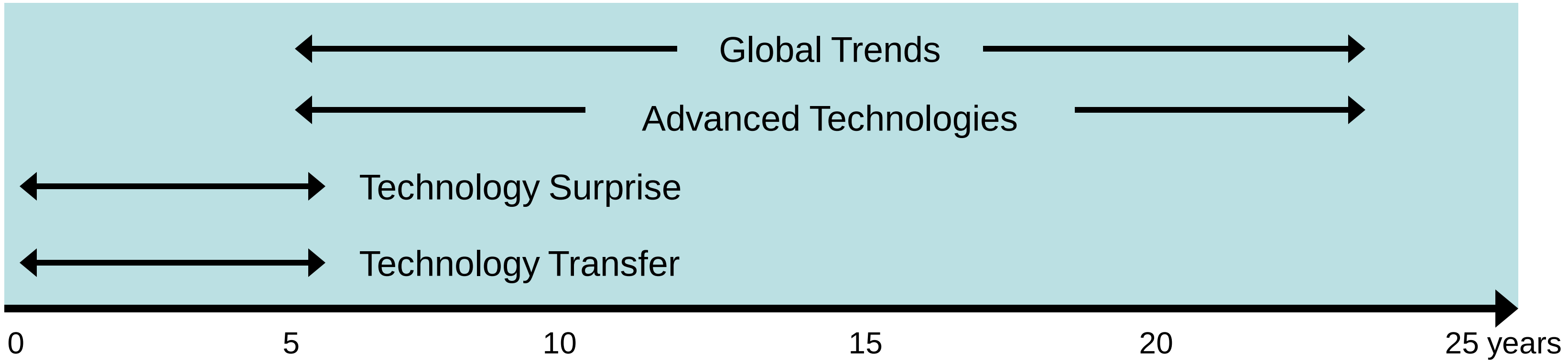
Follow-on Guidance

DNI Strategic Plan (MO5): …anticipate developments of strategic concern & identify opportunities as well as vulnerabilities for decision makers.

Defense Intelligence Analysis Program: Create, enhance, & sustain the capability to understand & enunciate S&T advances that might transition to, or transform military capabilities.

Current Org – Defense Warning Office

- Analyze long-term (5-25 years) defense-related economic, social, political, scientific, & technical trends.
- Identify near-term (now-5 yrs) obscure, ambiguous, or unforeseen threats.



DWO-1
Foreign Materiel Division

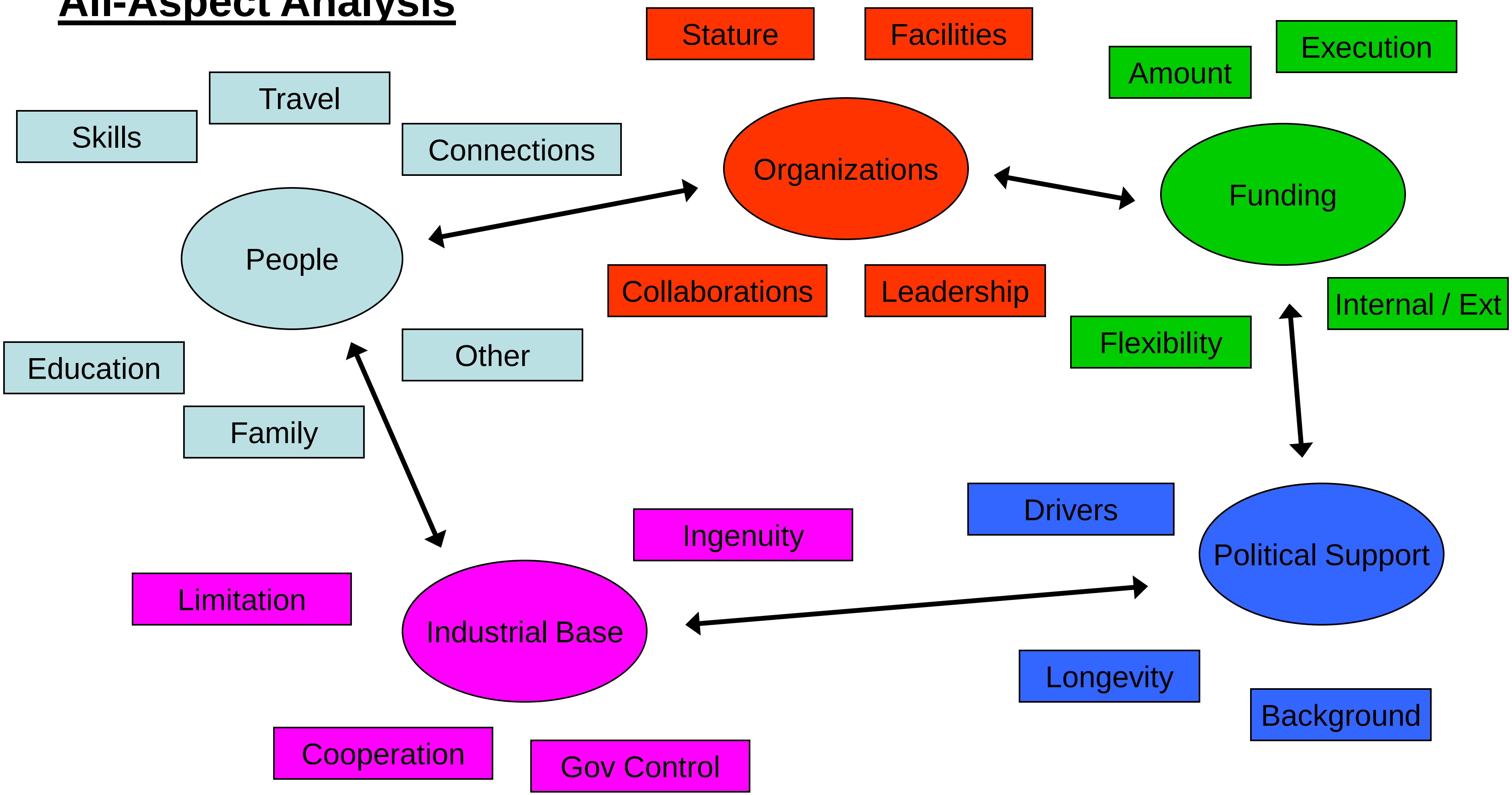
DWO-2
Strategic Plans & Assessments

DWO-3
Acquisition Support Division

DWO-4
Technology Warning Division

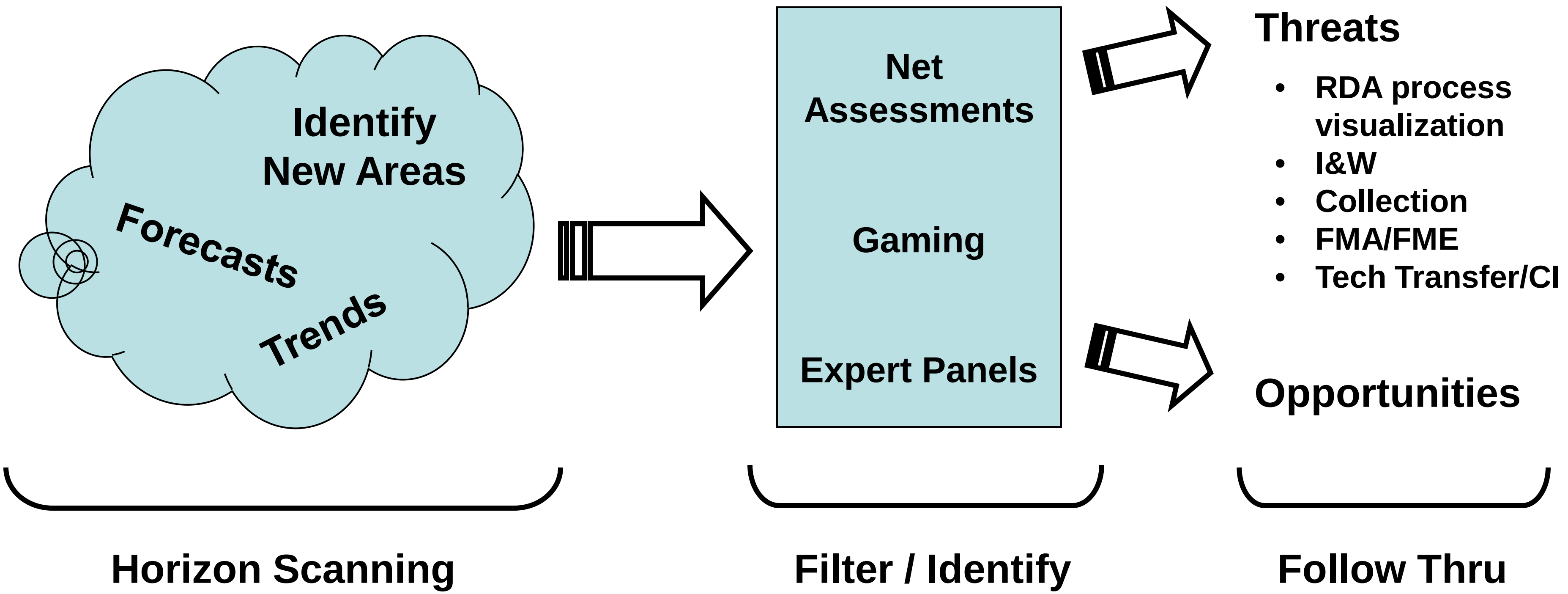
Future Capabilities

All-Aspect Analysis



Future Capabilities

<u>Integrated Processes</u>



Partnering Opportunities

- **Expertise**
  - Industry as a partner not a producer
  - Knowledge transfer
  - Continuing education
  - Career entanglement

- **Processes**
  - Knowledge management
  - Open source exploitation best practices
  - Horizon scanning
  - Production paradigm guidance
  - M&S plug & play

Questions?

Dr. Don Wyma

Director for Scientific & Technical Intelligence Analysis

Office of the Under Secretary of Defense (Intelligence)

donald.wyma@osd.mil

703-602-1426